



NEOTERIS

NEOTERIS INSTANT VIRTUAL EXTRANET

**Administrationshandbuch**



# **NEOTERIS INSTANT VIRTUAL EXTRANET**

## **Administrationshandbuch**

©2001-2003 Neoteris, Inc. Alle Rechte vorbehalten.

Alle Information in diesem Dokument sind Eigentum von Neoteris, Inc. Dieses Dokument kann ohne vorherige Ankündigung geändert werden. Es kann jederzeit durch andere Dokumente aktualisiert, ersetzt oder außer Kraft gesetzt werden.

Die in diesem Dokument enthaltenen Beschreibungen bedeuten nicht, dass Lizenzen gewährt werden, um erforderliche Technologien zum Implementieren von Systemen oder Komponenten, die dieser Spezifikation entsprechen, herzustellen, zu nutzen, zu verkaufen, zu lizenzieren oder auf sonstige Weise weiterzugeben. Neoteris, Inc. äußert sich in keiner Weise hinsichtlich bestehender oder zukünftiger Patentrechte, Copyrights, Marken, Geschäftsgeheimnisse oder anderer proprietärer Rechte für die in dieser Spezifikation beschriebenen Technologien.

Neoteris, Inc. schließt alle anderen Garantien, gleich ob ausdrücklich oder konkludent, einschließlich, jedoch nicht beschränkt auf konkludente Garantien der Handelsüblichkeit oder Eignung für einen bestimmten Zweck aus.

Neoteris, Inc.  
940 Stewart Drive  
Sunnyvale, CA 94085  
USA  
Telefon: 408-962-8200  
Fax: 408-962-8201

Wenn Sie weitere Informationen erhalten möchten, senden Sie eine E-Mail an die folgende Adresse:  
[help@support.neoteris.com](mailto:help@support.neoteris.com)

Teilenummer: 101-1001-001 C (072203 cay)

# Inhalt

<b>Kapitel1. Einführung in die Neoteris IVE-Appliance.....</b>	<b>1</b>
<b>Was ist IVE? .....</b>	<b>1</b>
<b>Wie funktioniert das IVE? .....</b>	<b>2</b>
<b>Welchen Leistungsumfang bietet das IVE? .....</b>	<b>3</b>
 <b>Kapitel2. Verwalten von systemweiten Einstellungen.....</b>	 <b>5</b>
<b>System &gt; Menü „Settings“ .....</b>	<b>5</b>
Anzeigen des Systemstatus, Neustart, Herunterfahren und Senden eines	
Ping-Befehls an verbundene Server .....	6
Eingeben oder Aktualisieren der Systemlizenz .....	7
Ändern systemweiter Sicherheits- und Leistungseinstellungen .....	9
Festlegen von Regeln für die Zwischenspeicherung von Inhalten .....	13
Einstellen der Systemzeit .....	16
Einstellen, Anzeigen, Löschen und Speichern des Systemprotokolls .....	18
Anzeigen der Systemstatistik .....	22
Planen der Archivierung von Systeminformationen .....	24
Aufzeichnen einer Ablaufverfolgungsdatei zu Debuggingzwecken .....	26
Erstellen eines Snapshots des IVE-Systemstatus. ....	27
Abhören von Netzwerkpaketheadern mit einem Sniffer-Programm .....	28
Ausführen eines ARP-, ping-, traceroute- oder nslookup-Befehls .....	30
Aktivieren von Remotedebugging für den Neoteris-Support .....	31
Festlegen systemweiter Anmeldeeinschränkungen .....	32
Festlegen systemweiter Anmeldeoptionen .....	33
Festlegen der Codierung für die Internationalisierung .....	35
<b>System &gt; Menü „Appearance“ .....</b>	<b>36</b>
Anpassen der Darstellung des IVE .....	36
Anpassen der IVE-Anmeldeseite .....	38
<b>System &gt; Menü „Certificates“ .....</b>	<b>41</b>
Importieren eines bestehenden Serverzertifikats und eines privaten Schlüssels .....	43

Importieren eines erneuerten Serverzertifikats, für das der bestehende privater Schlüssel verwendet wird .....	45
Erstellen einer Zertifikatssignaturanforderung für ein neues Serverzertifikat .....	47
Importieren eines signierten Serverzertifikats, das anhand einer Zertifikatssignaturanforderung erstellt wurde .....	50
Importieren eines Stammzertifikats zur Überprüfung eines clientseitigen Zertifikats .....	52
Importieren eines Codesignaturzertifikats .....	55
<b>System &gt; Menü „Import/Export“ .....</b>	<b>58</b>
Exportieren einer Systemkonfigurationsdatei .....	58
Importieren einer Systemkonfigurationsdatei .....	59
Exportieren lokaler Benutzerkonten .....	60
Importieren lokaler Benutzerkonten .....	61
Exportieren von ACLs und Lesezeichen .....	64
Importieren von ACLs und Lesezeichen .....	64
<b>System &gt; Menü „Install Service Package“ .....</b>	<b>66</b>
Installieren eines Neoteris-Softwaredienstpakets .....	66
<b>System &gt; Menü „Secure Meetings“ .....</b>	<b>67</b>
Aktivieren von E-Mail-Benachrichtigungen für Konferenzen .....	68
Anzeigen und Absagen geplanter Konferenzen .....	70
 <b>Kapitel3. Verwalten der Authentifizierung und Autorisierung für IVE .....</b>	 <b>71</b>
<b>Übersicht über Authentifizierung und Autorisierung .....</b>	<b>72</b>
<b>Unterstützte Authentifizierungsserver .....</b>	<b>75</b>
Lokaler IVE-Authentifizierungsserver .....	75
Active Directory oder Windows NT-Domäne .....	75
LDAP-Server .....	76
NIS-Server .....	76
RADIUS-Server .....	77
ACE/Server .....	78
Netegrity SiteMinder-Server .....	79
<b>Authentication &amp; Authorization &gt; Menü „Administrators“ .....</b>	<b>82</b>
Erstellen, Löschen, Bearbeiten und Suchen von Administratorengruppenkonten .....	82
Festlegen von Zeitbegrenzungen für Administratorengruppensitzungen .....	86
Festlegen eines Servers für die Authentifizierung der Administratorengruppe .....	87

Festlegen von IP-Adresseinschränkungen für die Administratorengruppe .....	89
Angeben von Zertifikatanforderungen für die Administratorengruppe .....	91
<b>Authentication &amp; Authorization &gt; Menü „Authentication Servers“ .....</b>	<b>92</b>
Definieren einer Authentifizierungsserverinstanz .....	92
Schritt 1: Angeben von Serverinformationen und der Option für die Zuordnung von Benutzern zu Gruppen .....	92
Konfigurieren eines Servers für das Gruppenlookup .....	97
Schritt 2: Angeben von Informationen für die Gruppenzuordnung .....	98
Schritt 3: Erstellen lokaler Benutzer (nur bei lokaler IVE-Authentifizierung) .....	101
Schritt 4: Delegieren von Benutzerverwaltungsrechten (nur bei lokaler IVE-Authentifizierung) .....	104
Delegieren von Benutzerverwaltungsrechten an Endbenutzer .....	104
<b>Ergänzende Informationen zur Konfiguration von Authentifizierungsservern .....</b>	<b>106</b>
Definieren einer Active Directory-Serverinstanz oder einer Windows NT-Domänenserverinstanz .....	106
Festlegen einer LDAP-Serverinstanz .....	108
Festlegen einer NIS-Serverinstanz .....	112
Festlegen einer RADIUS-Serverinstanz .....	113
Festlegen einer ACE/Serverinstanz .....	116
Generieren einer ACE/Agent-Konfigurationsdatei .....	117
Festlegen einer Netegrity SiteMinder-Instanz .....	119
Konfigurieren des IVE als Web-Agent auf einem SiteMinder-Richtlinienserver .....	123
<b>Menü „Authentication &amp; Authorization &gt; Authorization Groups“ .....</b>	<b>126</b>
Überprüfen einer Zusammenfassung der Einstellungen für Autorisierungsgruppen .....	127
Übersicht über Network Connect .....	129
Aktivieren und Konfigurieren Network Connect .....	130
Angeben von Zeitbegrenzungen und Roamingfunktionen für Autorisierungsgruppen .....	133
Angeben von Benutzeranmeldeinformationen und der Beständigkeit von IVE-Sitzungscookies .....	135
Überprüfen der Zuordnungen von Servern zu Gruppen .....	137
Einschränken der möglichen IP-Adressen für die Benutzeranmeldung .....	138
Einschränken der möglichen Browser für die Benutzeranmeldung .....	139
Festlegen, dass Clientcomputer über ein gültiges Zertifikat verfügen müssen .....	142
Durchführen einer clientseitigen Überprüfung der Software für die Endpunktsicherheit .....	145
Festlegen von allgemeinen Einstellungen für Webbrowsing .....	148
Konfigurieren von Hosts für die Option zum selektiven Neuschreiben .....	152

Aktivieren und Angeben von Einstellungen für den Durchgangssproxy .....	153
Zugriffssteuerung für Webressourcen .....	158
Erstellen von Lesezeichen für Webressourcen .....	161
Angeben der Server, mit denen Java-Applets eine Verbindung herstellen können .....	163
Steuern des Netzwerkzugriffs unter Windows und UNIX/NFS .....	164
Zugriffssteuerung für Windows-Ressourcen .....	167
Erstellen von Lesezeichen für Windows-Ressourcen .....	170
Zugriffssteuerung für UNIX/NFS-Ressourcen .....	172
Erstellen von Lesezeichen für UNIX-Ressourcen .....	174
Aktivieren der Aktualisierungsoption für den Secure Email Client .....	176
Angeben von allgemeinen Client-/Server-Anwendungseinstellungen .....	178
Zusätzliche Optionen bei aktiviertem J-SAM .....	181
Erstellen von Lesezeichen für sichere Terminalsitzungen .....	185
Übersicht über Windows Secure Application Manager (W-SAM) .....	187
Festlegen von Anwendungen und Hosts, die mit W-SAM gesichert werden sollen. ....	189
Übersicht über Java Secure Application Manager (J-SAM) .....	193
Festlegen von Clientanwendungen, für die J-SAM eine Portweiterleitung durchführt .....	197
Konfigurieren der externen DNS-Server und Benutzercomputer (falls erforderlich) .....	201
Konfigurieren eines PCs, der die Verbindung mit dem IVE über einen Proxywebserver herstellt .....	202
Testen von J-SAM im Unternehmen .....	203
Erweiterte Unterstützung für MS Exchange .....	205
Angeben zulässiger MS Exchange-Server .....	207
Erweiterte Unterstützung für Lotus Notes .....	210
Festlegen zulässiger Lotus Notes-Server .....	211
Konfigurieren des Lotus Notes-Clients .....	213
Erweiterte Unterstützung für Citrix NFuse .....	214
Ändern von Citrix NFuse-Standardeinstellungen .....	215
Ermöglichen und Konfigurieren von Konferenzen für Autorisierungsgruppen .....	216
<b>Authentication &amp; Authorization &gt; Menü „Import Users“ .....</b>	<b>220</b>
Erstellen einer Textdatei mit Benutzerdatensätzen .....	220
Importieren von Benutzer- und Gruppeneinstellungen auf einen Authentifizierungsserver .....	222
<b>Authentication &amp; Authorization &gt; Menü „Active Users“ .....</b>	<b>223</b>
Überwachen von am IVE angemeldeten Benutzern .....	223



<b>Kapitel 4. Verwalten von IVE Netzwerkeinstellungen</b>	225
<b>Konfigurieren allgemeiner Netzwerkeinstellungen für das IVE</b>	226
<b>Konfigurieren eines Clusters von IVE-Servern</b>	227
Übersicht über Cluster	228
Bereitstellen eines Clusters im Aktiv/Passiv-Modus	229
Bereitstellen eines Clusters im Aktiv/Aktiv-Modus	230
Statussynchronisierung	232
<b>Konfigurieren des IVE als Webproxy</b>	233
<b>Konfigurieren der Aktualisierungsoption für Secure Email Client</b>	234
Auswählen eines E-Mail-Clients	235
Arbeiten mit einem standardbasierten Mailserver	236
Arbeiten mit Microsoft Exchange Server	236
Arbeiten mit Lotus Notes und Lotus Notes Mail Server	239
<b>Überwachen des IVE als SNMP-Agent</b>	239
<b>Network &gt; Menü „Network Settings“</b>	240
Ändern von Netzwerkeinstellungen für den internen Port (LAN-Schnittstelle)	240
Aktivieren des externen Ports (DMZ-Schnittstelle)	241
Angaben von statischen Routen für den Netzwerkverkehr	243
Angaben von Hostnamen, die vom IVE lokal aufgelöst werden sollen	245
<b>Network &gt; Menü „Clustering“</b>	247
Definieren und Initialisieren eines Clusters	247
Hinzufügen eines IVEs zu einem Cluster über die serielle Konsole	249
Hinzufügen eines IVEs zu einem Cluster über die Administrator-Konsole	254
Aktualisieren eines Clusters	256
Verwalten von Clusterknoten und Angeben neuer Clustermitglieder	257
Ändern von Clustereigenschaften oder Löschen eines Clusters	262
<b>Menü „Network &gt; Web Proxy“</b>	264
Angaben eines Webproxys	264
<b>Menü „Network &gt; Email Settings“</b>	267
Festlegen von IMAP/POP/SMTP-Mailservern und von Einstellungen für die Benutzerauthentifizierung	267
<b>Menü „Network &gt; SNMP“</b>	270

**Anhang A. Verwenden der seriellen Konsole von Neoteris.....273**

Herstellen einer Verbindung mit der seriellen Konsole des IVE .....273

Rollback zu einem vorherigen Systemzustand .....274

Zurücksetzen des Neoteris-Geräts auf die Werkseinstellungen .....277

Durchführen gängiger Wiederherstellungsvorgänge .....280

# Elemente der Benutzeroberfläche

## Systemmenüs

<b>System &gt; Menü „Settings“</b> .....	5
Registerkarte „General“ .....	6
Registerkarte „License“ .....	7
Security > Unterregisterkarte „General“ .....	9
Security > Unterregisterkarte „Content Caching“ .....	13
Registerkarte „Time“ .....	16
Log > Unterregisterkarte „View“ .....	18
Log > Unterregisterkarte „Settings“ .....	18
Registerkarte „Statistics“ .....	22
Registerkarte „Archiving“ .....	24
Debugging > Unterregisterkarte „Trace“ .....	26
Debugging > Unterregisterkarte „State“ .....	27
Debugging > Unterregisterkarte „TCP Dump“ .....	28
Debugging > Unterregisterkarte „Commands“ .....	30
Debugging > Unterregisterkarte „Remote Debugging“ .....	31
Sign-in Options > Unterregisterkarte „Restrictions“ .....	32
Sign-in Options > Unterregisterkarte „Authorization Mode“ .....	33
<b>System &gt; Menü „Appearance“</b> .....	36
Registerkarte „General“ .....	36
Registerkarte „Sign-in Page“ .....	38
<b>System &gt; „Certificates“ (Menü)</b> .....	41
Registerkarte „Server Certificate“ .....	42
Registerkarte „CA Certificate“ .....	52
Registerkarte „Applet Certificate“ .....	54
<b>System &gt; Menü „Import/Export“</b> .....	58
Registerkarte „Configuration“ .....	58
Registerkarte „User Accounts“ .....	60
Registerkarte „ACLs & Bookmarks“ .....	62
<b>System &gt; Menü „Install Service Package“</b> .....	66
<b>System &gt; Menü „Secure Meetings“</b> .....	67
Registerkarte „General“ .....	68

Registerkarte „Schedule“ .....	70
--------------------------------	----

## Menüs „Authentication & Authorization“

<b>Authentication &amp; Authorization &gt; Menü „Administrators“ .....</b>	<b>82</b>
Registerkarte „Members“ .....	82
Registerkarte „Session“ .....	86
Authentication > Unterregisterkarte „Authentication Server“ .....	87
Authentication > Unterregisterkarte „Address Restrictions“ .....	89
Authentication > Unterregisterkarte „Certificate“ .....	91
<b>Authentication &amp; Authorization &gt; Menü „Authentication Servers“ .....</b>	<b>92</b>
<b>Menü „Authentication &amp; Authorization &gt; Authorization Groups“ .....</b>	<b>126</b>
General > Unterregisterkarte „Overview“ .....	127
General > Unterregisterkarte „Network Connect“ .....	129
General > Unterregisterkarte „Session“ .....	133
General > Unterregisterkarte „Options“ .....	135
Authentication > Unterregisterkarte „Authentication Server“ .....	137
Authentication > Unterregisterkarte „Address Restrictions“ .....	138
Authentication > Unterregisterkarte „Browser Restrictions“ .....	139
Authentication > Unterregisterkarte „Certificate“ .....	142
Authentication > Unterregisterkarte „Certificate“ .....	144
Web > Unterregisterkarte „General“ .....	148
Web > Unterregisterkarte „Access Control“ .....	158
Web > Unterregisterkarte „Bookmarks“ .....	161
Web > Unterregisterkarte „Java Socket ACL“ .....	163
Files > Unterregisterkarte „General“ .....	164
Files > Unterregisterkarte „Windows Access“ .....	167
Files > Unterregisterkarte „Windows Bookmarks“ .....	170
Files > Unterregisterkarte „UNIX Access“ .....	172
Files > Unterregisterkarte „UNIX Bookmarks“ .....	174
Registerkarte „Email Client“ .....	176
Applications > Unterregisterkarte „General“ .....	178
Applications > Unterregisterkarte „Terminal Sessions“ .....	185
Applications > Unterregisterkarte „Secure Application Manager (W-SAM)“ .....	187
Applications > Unterregisterkarte „Secure Application Manager (J-SAM)“ .....	193
Applications > Unterregisterkarte „MS Exchange (J-SAM)“ .....	205
Applications > Unterregisterkarte „Lotus Notes (J-SAM)“ .....	210
Applications > Unterregisterkarte „Citrix NFuse (J-SAM)“ .....	214
Registerkarte „Meetings“ .....	216

<b>Authentication &amp; Authorization &gt; Menü „Active Users“</b> .....	220
<b>Authentication &amp; Authorization &gt; Menü „Active Users“</b> .....	223

## **Menü „snetwork Settings“**

Registerkarte „Internal Port“ .....	240
Registerkarte „External Port“ .....	241
Registerkarte „Static Routes“ .....	243
Registerkarte „Hosts“ .....	245
<b>Menü „Network &gt; Clustering“</b> .....	247
Registerkarte „Status“ .....	257
Registerkarte „Properties“ .....	262
<b>Menü „Network &gt; Web Proxy“</b> .....	264
<b>Menü „Network &gt; Email Settings“</b> .....	267
<b>Menü „Network &gt; SNMP“</b> .....	270



---

# Vorwort

In diesem Handbuch finden Sie die erforderlichen Informationen zum Konfigurieren und Verwalten des Neoteris Instant Virtual Extranet (IVE), unter anderem:

- Eine allgemeine Übersicht, um die Funktionen des Geräts kennen zu lernen
- Schrittweise Anleitungen zum Installieren und Konfigurieren des Neoteris IVE-Server
- Anweisungen zum Durchführen der Systemverwaltung

---

## Zielgruppe

Dieses Handbuch wendet sich an Systemadministratoren, die für die Installation und Konfiguration einer Neoteris IVE-Appliance zuständig sind.

---

## Weiterführende Informationen

Wenn Sie bei der Installation Hilfe benötigen, schreiben Sie eine E-Mail an die Adresse „[help@support.neoteris.com](mailto:help@support.neoteris.com)“, oder füllen Sie unter „<http://support.neoteris.com>“ ein Supportformular aus.

Ein Software-Servicepaket erhalten Sie unter „<http://support.neoteris.com>“.

Informationen über das Aktualisieren der Konfiguration finden Sie unter „[www.neoteris.com](http://www.neoteris.com)“, oder schreiben Sie eine E-Mail an „[sales@neoteris.com](mailto:sales@neoteris.com)“.





---

## Kapitel1

# Einführung in die Neoteris IVE-Appliance

Mit der Neoteris IVE-Appliance (Instant Virtual Extranet) können Sie Mitarbeitern, Partnern und Kunden über einen beliebigen Webbrowser überall einen sicheren und gesteuerten Zugriff auf die Dateiserver und Webserver des Unternehmens, auf systemeigene Nachrichten- und E-Mail-Clients, auf gehostete Server und vieles mehr geben!

---

## Was ist IVE?

Das IVE von Neoteris ist eine so genannte Netzwerkappliance, die stabile Sicherheit bietet, indem sie als Zwischenglied für die Datenströme fungiert, die zwischen externen Benutzern und internen Ressourcen übertragen werden. Zu diesen gehören:

- MS Terminal-Server
- MS Exchange-Server
- Lotus Notes-Server
- Internet-E-Mail-Server
- Terminal-basierte Anwendungen (IBM 3270, VT100)
- Dokumente auf Dateiservern
- Webbasierte Unternehmensanwendungen
- Intranetseiten

Durch das Neoteris IVE wird es überflüssig, in einem herkömmlichen DMZ Toolkits für Extranets bereitzustellen oder den Mitarbeitern ein VPN (Virtual Private Network) für Remotezugriffe zur Verfügung zu stellen. Das IVE vermittelt zwischen externen Verbindungen, über die es sichere Anforderungen erhält, und internen Ressourcen, an die es Anforderungen für authentifizierte Benutzer sendet.

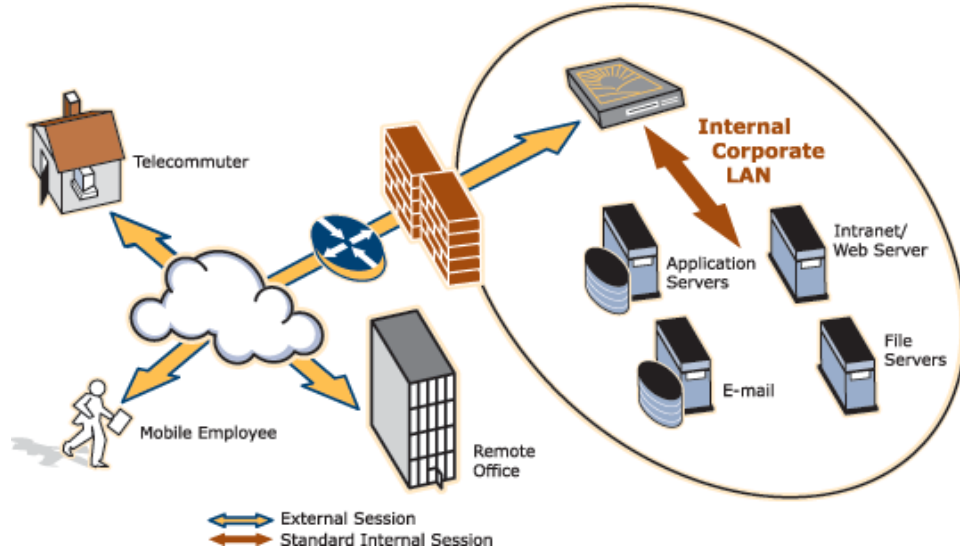


Abbildung 1: Die Neoteris IVE-Appliance innerhalb eines LAN

---

## Wie funktioniert das IVE?

Das IVE von Neoteris fungiert als sicheres Gateway auf Anwendungsebene, das sämtliche Anforderungen zwischen dem öffentlichen Internet und internen Unternehmensressourcen vermittelt. Auf sämtliche Anforderungen, die das IVE erhält, wurde bereits durch den Browser des Endbenutzers eine 128-Bit-SSL/HTTPS-Verschlüsselung angewendet. Unverschlüsselte Anforderungen werden verworfen. Jede Anforderung wird einer vom Administrator definierten Zugriffssteuerung unterzogen und unterliegt Autorisierungsrichtlinien, beispielsweise einer 2-Faktor-Authentifizierung oder clientseitigen digitalen Zertifikaten, bevor sie an die internen Ressourcen weitergeleitet wird. Da das IVE eine stabile Sicherheitsschicht zwischen dem öffentlichen Internet und den internen Ressourcen zur Verfügung stellt, müssen Administratoren nicht fortwährend Sicherheitsrichtlinien verwalten und Sicherheitslücken für zahlreiche verschiedene Anwendungen und Webserver beheben, die in dem öffentlichen DMZ bereitgestellt werden.

Das IVE vermittelt den Zugriff auf mehrere Arten von Anwendungen und Ressourcen mit Hilfe von einfachen Webbrowsertechnologien. Die Benutzer erhalten über eine durch das Neoteris IVE gehostete Extranetsitzung einen authentifizierten Zugriff auf autorisierte Ressourcen. Sie können über einen beliebigen, mit dem Internet verbundenen Webbrowser auf umfangreiche webbasierte Unternehmensanwendungen, auf Java-Anwendungen, Dateifreigaben und Terminalhosts zugreifen. Außerdem können die Benutzer, die über einen Laptop der Firma und über Client-/Serveranwendungen wie Microsoft Outlook oder Lotus Notes verfügen, durch Proxyaktivierung über dieselbe sichere Websitzung auf Anwendungen zugreifen.

---

## Welchen Leistungsumfang bietet das IVE?

Die Neoteris Access™ Series-Produktfamilie bietet ein hohes Maß an Skalierbarkeit für Unternehmen, eine hohe Verfügbarkeit sowie Sicherheitsfunktionen, um den sicheren Zugriff auf Netzwerkressourcen zu erweitern. In nur wenigen Stunden können Sie den Benutzern einen sicheren Zugriff auf die folgenden Elemente ermöglichen:

- Interne Unternehmenswebsites und webbasierte Anwendungen, darunter clientseitige Java-Applets, unter Verwendung von Desktopcomputern, Laptopcomputern und drahtlosen Pocket PC-Geräten (Standard)
- Interne Dateiserver (NFS und CIFS) des Unternehmens sowie Funktionen zur Dateiübertragung an und von beliebigen Verzeichnissen (Standard)
- Systemeigene Nachrichtenclients wie Microsoft Outlook und IBM/Lotus Notes von jedem PC aus (Aktualisierungsoption für Secure Email Client)
- Auf Standards basierende E-Mail-Clients wie Microsoft Outlook Express, Netscape Communicator und Eudora von Qualcomm von jedem PC aus (Aktualisierungsoption für Secure Application Manager)
- Client-/Serveranwendungen wie Citrix ICA Client, pcAnywhere und MS-Terminaldienste von jedem PC aus (Aktualisierungsoption für Secure Application Manager)
- Gehostete Server über Telnet und SSH von jedem PC aus (Aktualisierungsoption für Secure Terminal Access)
- Funktionen für die sichere Zusammenarbeit, einschließlich der Planung von Konferenzen, Remotekonferenzvorführungen, Remotesteuerung des Desktops des Vorführenden sowie Textchats (Option in Secure Meeting)

Ihre Mitarbeiter, Partner und Kunden benötigen lediglich einen Standard-webbrowser für den PC (Internet Explorer/Netscape/AOL/Pocket IE) und eine Internetverbindung für den Zugriff auf die intuitive IVE-Startseite. Auf dieser Seite wird das Fenster bereitgestellt, über das die Benutzer sicher Web- oder Dateiserver durchsuchen, HTML-fähige Unternehmensanwendungen verwenden, den Client-/Serveranwendungsproxy starten oder eine Terminalsitzung beginnen können<sup>1</sup>.

Die Installation, Konfiguration und Verwaltung des IVE sind unkompliziert. Bei dem IVE handelt es sich um eine Netzwerkappliance, die innerhalb weniger Minuten im Rack montiert werden kann. Sobald eine Verbindung mit Ihrem Netzwerk besteht, müssen Sie an der seriellen Konsole nur noch einige anfängliche System- und Netzwerkeinstellungen eingeben, um den Zugriff auf die Administratorkonsole zu erhalten. Die Administratorkonsole ist die webbasierte Schnittstelle, über die Sie das IVE den Anforderungen Ihres Unternehmens entsprechend konfigurieren und verwalten können. Die folgenden Features ermöglichen eine problemlose Bereitstellung und effiziente Wartung des Systems:

- Einfache Serverintegration—Das IVE lässt sich in vorhandene Authentifizierungsserver (LDAP, RADIUS, NIS, Windows NT-Domäne, Active Directory und RSA-ACE/Server) des Unternehmens integrieren. Sie müssen keine Änderungen an den internen Webservern, Dateiservern oder Netzwerken vornehmen.
- Zertifikatauthentifizierung—Schützt Anwendungen ohne Änderungen an den internen Ressourcen. Sie wählen lediglich die digitalen Zertifikate als Teil des Authentifizierungsschemas für das IVE aus (Aktualisierungsoption für clientseitige digitale Zertifikate).
- Hohe Verfügbarkeit und Redundanz—Keine Ausfallzeit für die Benutzer im seltenen Fall eines Systemausfalls und „Stateful Peering“, durch das die Benutzereinstellungen, die Systemeinstellungen und die Sitzungsdaten der Benutzer synchronisiert werden (Aktualisierungsoption für Cluster).
- Einfache Firewallrichtlinien—Von außen ist nur ein SSL-Zugriff auf die Neoteris IVE-Appliance erforderlich.
- Gruppenbasierte Zugriffssteuerung auf Datei- und URL-Ebene (Standard für Access 3000- und Access 5000-Systeme).
- Zentralisierte Protokollierung auf Anwendungsebene, durch die Administrator- und Benutzeraktionen, Verbindungs-, Datei- und Webanforderungen sowie Systemfehler verfolgt werden.
- Systemsoftwareaktualisierungen über das Internet.
- SNMP- und DMZ-Unterstützung.

---

1. Welche Funktionen zur Verfügung stehen, hängt von dem erworbenen Produkt der Neoteris Access Series und den Aktualisierungsoptionen ab.

## Kapitel2

# Verwalten von systemweiten Einstellungen

Die Verwaltung des IVE umfasst die Konfiguration und Verwaltung von systemweiten Einstellungen, Authentifizierungsservern, Autorisierungsgruppen und Netzwerkeinstellungen. In diesem Kapitel werden die systemweiten Verwaltungsaufgaben und -einstellungen beschrieben, die alle IVE-Endbenutzer betreffen und die Sie über die **System**-Menüs konfigurieren können:

System > Menü „Settings“ .....	5
System > Menü „Appearance“ .....	36
System > Menü „Certificates“ .....	41
System > Menü „Import/Export“ .....	58
System > Menü „Install Service Package“ .....	66
System > Menü „Secure Meetings“ .....	67

## System > Menü „Settings“

Auf den Registerkarten des Menüs **System > Settings** können Sie die folgenden systembezogenen Aufgaben durchführen:

- Anzeigen des Systemstatus, Neustart, Herunterfahren und Senden eines Ping-Befehls an verbundene Server (6)
- Eingeben oder Aktualisieren der Systemlizenz (7)
- Ändern systemweiter Sicherheits- und Leistungseinstellungen (9)
- Einstellen der Systemzeit (16)
- Einstellen, Anzeigen, Löschen und Speichern des Systemprotokolls (18)
- Anzeigen der Systemstatistik (22)
- Planen der Archivierung von Systeminformationen (24)
- Aufzeichnen einer Ablaufverfolgungsdatei zu Debuggingzwecken (26)
- Erstellen eines Snapshots des IVE-Systemstatus. (27)

- Abhören von Netzwerkpaketheadern mit einem Sniffer-Programm (28)
- Ausführen eines ARP-, ping-, traceroute- oder nslookup-Befehls (30)
- Aktivieren von Remotedebugging für den Neoteris-Support (31)
- Festlegen systemweiter Anmeldeeinschränkungen (32)
- Festlegen systemweiter Anmeldeoptionen (33)
- Festlegen der Codierung für die Internationalisierung (35)

## Registerkarte „General“

### ☒ Anzeigen des Systemstatus, Neustart, Herunterfahren und Senden eines Ping-Befehls an verbundene Server

Wenn Sie sich an der Administratorkonsole anmelden, ist das Menü **System > Settings > General** ausgewählt, und die Seite **General** wird angezeigt. Auf dieser Seite sind die Details zum IVE-Server und den Systembenutzern zusammengefasst. Wenn Sie auf anderen Seiten Änderungen vornehmen, werden die entsprechenden Informationen auf der Seite **General** aktualisiert.

Auf dieser Seite können Sie auch die folgenden Aktionen durchführen

- Neoteris IVE-Server neu starten, wenn Sie auf **Reboot Now** klicken.
- Neoteris IVE-Server herunterfahren, wenn Sie auf **Shutdown** klicken. Der Server wird heruntergefahren, und Sie müssen an der Appliance Reset-Schalter drücken, um den Server neu zu starten. Beachten Sie, dass das Gerät nach dem Herunterfahren des Servers eingeschaltet bleibt.
- Senden Sie vom Neoteris IVE-Server einen ICMP-Ping-Befehl an alle Server, für deren Verwendung das IVE konfiguriert ist und deren Verbindungen gemeldet werden, wenn Sie auf **Servers Connectivity** klicken. Der Status der einzelnen Server wird unter **Notices** gemeldet.

Informationen zur Handhabung der folgenden Situationen finden Sie in „Anhang A: Verwenden der seriellen Konsole von Neoteris“ auf Seite 273:

- Sie haben Ihre Anmeldedaten vergessen.
- Sie haben die IP-Beschränkungen so eingestellt, dass Sie sich nicht mehr am Gerät anmelden können.
- Sie möchten das System in den vorherigen Zustand zurücksetzen.
- Sie müssen das System auf die Werkseinstellungen zurücksetzen.

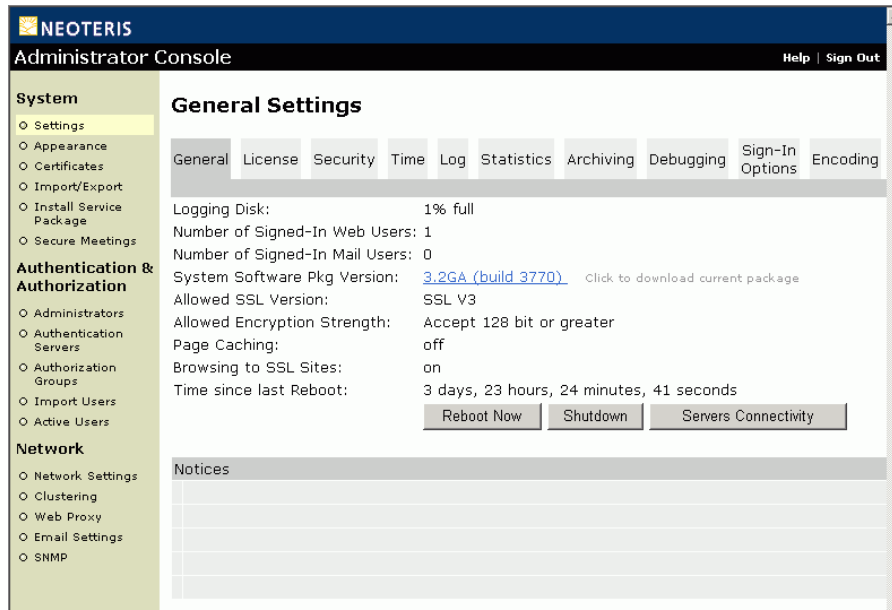


Abbildung 2: System > Settings > General

## Registerkarte „License“

### ☒ Eingeben oder Aktualisieren der Systemlizenz

Die Neoteris IVE-Appliance wird mit Hilfe verschiedener Optionen lizenziert. Diese werden durch die folgenden Faktoren bestimmt:

- Aktivierte Systemkapazität (d. h. die Anzahl der gleichzeitig angemeldeten Benutzer)
- Supportumfang des von Ihnen erworbenen Produkts
- Optionale aktivierte Funktionen (d. h. Gruppenzugriffssteuerungen, clientseitige digitale Zertifikate, sicheres E-Mail-Proxy, sichere Nachrichtenübermittlung, sicherer Terminalzugriff und sichere Client-/Serveranwendungen)

Die Neoteris IVE-Appliance wird mit einer Werkslizenz ausgeliefert, die Folgendes ermöglicht:

- Durchsuchen von Web-, Windows- und UNIX/NFS-Dateien
- Systemkapazität für zwei gleichzeitig angemeldete Benutzer und fünf lokale Benutzerkonten

Nach einer erfolgreichen Anmeldung an der Administratorkonsole müssen Sie die Lizenz eingeben, die Ihnen per E-Mail von Neoteris zugesendet wurde. Auf der Seite **License** können Sie den Lizenzcode für Ihre Site eingeben und verwalten. Lesen Sie in jedem Fall die Lizenzvereinbarung, auf die Sie über die Seite **License** zugreifen können, bevor Sie Ihre Lizenz senden. Bei der über die Seite **License** verfügbaren Lizenzvereinbarung handelt es sich um denselben Text, der während des ersten Setups an der seriellen Konsole angezeigt wird.

### **So geben Sie eine IVE-Lizenz ein oder aktualisieren Sie diese**

1. Klicken Sie in der Administratorkonsole auf die Registerkarte **System > Settings > License**.
2. Klicken Sie auf die Verknüpfung **license agreement**. Lesen Sie die Lizenzvereinbarung. Falls Sie mit den Bestimmungen einverstanden sind, fahren Sie mit dem nächsten Schritt fort.
3. Geben Sie den Firmennamen und den Lizenzschlüssel ein, und klicken Sie dann auf **Enter**.



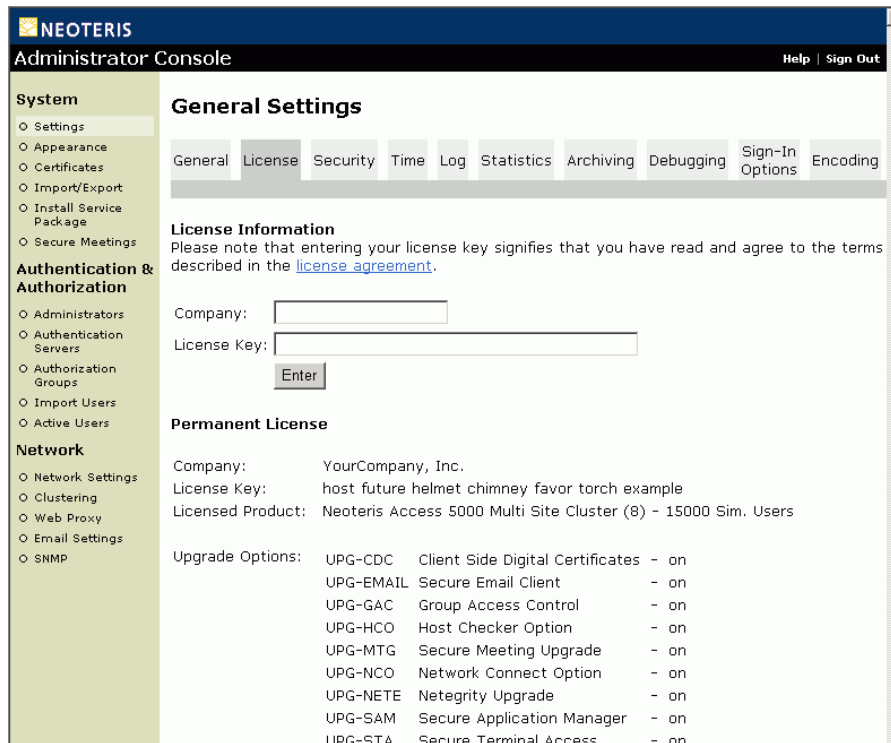


Abbildung 3: System > Settings > License

## Security > Unterregisterkarte „General“

### ☑ Ändern systemweiter Sicherheits- und Leistungseinstellungen

Über die Seiten des Menüs **Security** können Sie die standardmäßigen Sicherheitseinstellungen für den Neoteris IVE-Server ändern. Wir empfehlen, die Standardsicherheitseinstellungen zu verwenden, die höchste Sicherheit bereitstellen. Falls die Benutzer bestimmte Browser nicht verwenden oder auf bestimmte Webseiten nicht zugreifen können, müssen Sie diese Einstellungen jedoch möglicherweise ändern. Falls diese Probleme bei Benutzern auftreten, sollten sie eine Anpassung der folgenden Einstellungen in Erwägung ziehen:

- **Zulässige SSL- bzw. TLS-Version**

Für den Neoteris IVE-Server sind standardmäßig SSL, Version 3, und TLS erforderlich. In älteren Browsern wird SSL, Version 2, verwendet. Sie können entweder die Benutzer ihre Browser aktualisieren lassen oder die Einstellung ändern, damit sowohl SSL, Version 2, als auch SSL, Version 3, zulässig sind.

- **Zulässige Verschlüsselungsstärke**

Für den Neoteris IVE-Server ist in der Standardeinstellung eine 128-Bit-Verschlüsselung erforderlich. In älteren Browsern, die vor der Änderung des US-Exportgesetzes im Jahr 2000 entwickelt wurden, das bis dahin für den internationalen Export eine Verschlüsselungsstärke von 40 Bit vorschrieb, wird u. U. noch die 40-Bit-Verschlüsselung verwendet. Sie können entweder den Benutzern mitteilen, dass diese eine Aktualisierung auf einen Browser mit 128-Bit-Verschlüsselung vornehmen sollen, oder die erforderliche Verschlüsselungsstärke ändern, so dass auch die 40-Bit-Verschlüsselung zulässig ist.

- **Navigation zu SSL-Sites**

Der Neoteris IVE-Server gestattet die Navigation zu internen SSL-Sites (denen https:// vorangestellt ist) und akzeptiert als Standard sämtliche (temporären oder anderen) Zertifikate. Falls Sie Bedenken wegen Benutzern haben, die über IVE zu Sites ohne Zertifikate von einer gültigen externen Zertifizierungsstelle navigieren, deaktivieren Sie diese Funktion.

- **Vermittlung der Standardauthentifizierung**

Der Neoteris IVE-Server kann die Anmeldeinformationen von Benutzern vermitteln, um zu verhindern, dass ein Benutzer über die zwischengespeicherten Anmeldeinformationen eines anderen Benutzers auf Ressourcen zugreifen kann. Darüber hinaus kann das IVE die Anmeldeinformationen von Benutzern wiederverwenden und ermöglicht so eine Einzelanmeldung (Single Sign-In) für andere Intranetsites. Wenn Sie die Option für die Einzelanmeldung auswählen, stellt das IVE sicher, dass die Anmeldeinformationen nur innerhalb des Firmenintranets weitergeleitet werden.

- **Länge des Anmeldekennwortes**

Für das IVE müssen die auf der Anmeldeseite eingegebenen Benutzerkennwörter standardmäßig mindestens vier Zeichen lang sein. Für den zur Überprüfung der Anmeldeinformationen eines Benutzers verwendeten Authentifizierungsserver ist unter Umständen eine andere Mindestlänge erforderlich. Für die lokale Authentifizierungsdatenbank von IVE müssen die Benutzerkennwörter beispielsweise mindestens sechs Zeichen lang sein.

- **Automatische Versionsüberwachung**

Damit das System auf dem neuesten Stand und sicher bleibt, können Sie sich vom IVE automatisch über wichtige Softwarepatches und -aktualisierungen benachrichtigen lassen. Hierzu werden die folgenden Daten an Neoteris gemeldet: Ihr Firmenname, ein MD5-Hash Ihrer Lizenzeinstellungen sowie Informationen zur aktuellen Softwareversion (nähere Informationen finden Sie in der Dokumentation). Zum Schutz Ihres Systems wird dringend empfohlen, diesen automatischen Dienst zu aktivieren. Falls nötig, können Sie ihn jedoch auch deaktivieren.

Auf der Seite **Security > General** können Sie nicht nur Sicherheitseinstellungen konfigurieren, sondern zur Leistungssteigerung auch Beschleunigerkarten aktivieren. Beachten Sie, dass die folgenden Einstellungen nur angezeigt werden, wenn Sie ein A5000-IVE erworben haben, das mit der entsprechenden Karte ausgerüstet ist:

- **SSL-Beschleuniger**

Mit der SSL-Beschleunigerkarte wird die Leistung gesteigert, indem die Ver- und Entschlüsselung von SSL-Handshakes vom IVE an die Beschleunigerkarte delegiert wird.

- **ZIP-Beschleuniger**

Mit dem ZIP-Beschleuniger wird die Leistung gesteigert, indem alle HTML-, JavaScript- und CSS-Daten komprimiert werden, auf die per Navigation im Web oder im Dateisystem zugegriffen wird.

## **So ändern Sie die Sicherheits- und Leistungseinstellungen**

1. Wählen Sie in der Administratorkonsole die Registerkarte **System > Settings > Security > General**.
2. Wählen Sie die gewünschten Optionen aus, und klicken Sie dann auf **Save Changes**.

**NEOTERIS**

**Administrator Console**
[Help](#) | [Sign Out](#)

**System**

- Settings
- Appearance
- Certificates
- Import/Export
- Install Service Package
- Secure Meetings

**Authentication & Authorization**

- Administrators
- Authentication Servers
- Authorization Groups
- Import Users
- Active Users

**Network**

- Network Settings
- Web Proxy
- Email Settings
- SNMP

## General Settings

General | License | Security | Time | Log | Statistics | Archiving | Debugging | Sign-In Options | Encoding

General

Content Caching

### Allowed SSL and TLS Version

The older SSL V2 protocol has known security issues addressed by SSL V3 and TLS. Older browsers may only support SSL V2.

- ☒ Accept only SSL V3 and TLS (maximize security)
- ☐ Accept SSL V2 and V3 (maximize browser compatibility)

### Allowed Encryption Strength

Stronger ciphers improve the security of SSL encryption. Some browsers may only support 40-bit ciphers.

- ☐ Accept only 168-bit and greater (maximize security)
- ☒ Accept only 128-bit and greater (security and browser compatibility)
- ☐ Accept 40-bit and greater (maximize browser compatibility)

### Browsing to SSL Sites

This appliance supports browsing to SSL protected Web sites, but the site certificate will not be validated. If you have concerns about the validity of the site certificate, disable this capability.

- ☒ Enable browsing to SSL sites (maximize supported sites)
- ☐ Disable browsing to SSL sites (maximize security)

### Basic Authentication Intermediation

Browsers cache basic authentication credentials, possibly allowing users to access resources through a shared browser using another user's credentials. The IVE can intermediate basic authentication to prevent this.

- ☒ Enable intermediation (maximize security)
- ☐ Enable intermediation AND single sign-on for intranet sites (security and convenience)
- ☐ Disable intermediation (standard browser behavior, not recommended)

### Sign-in Password Length

You can require user passwords for signing in to the IVE to have a minimum length.

Minimum password length  characters

### Automatic Version Monitoring

To keep your system current and secure, the IVE can automatically notify you about critical software patches and updates. To do this, it reports to Neoteris the following data: your company name, an MD5 hash of your license settings, and information describing the current software version (for more information, refer to the documentation). For your protection, we strongly recommend that you enable this automatic service, but if necessary, you can disable it.

- ☒ Enabled
- ☐ Disabled

### SSL Accelerator

Here you can disable or enable SSL Accelerator card.

Abbildung 4: System > Settings > Security > General

## Security > Unterregisterkarte „Content Caching“

### ☒ Festlegen von Regeln für die Zwischenspeicherung von Inhalten

Die Zwischenspeicherung im Browser ist standardmäßig deaktiviert, so dass das IVE sämtliche Seiten, die für Remotebenutzer bereitgestellt werden, als nicht zwischenspeicherungs-fähig markiert. Durch diese Einstellung wird verhindert, dass vertrauliche Seiten auf Remotecomputern verbleiben, nachdem ein Benutzer den Browser geschlossen hat. Diese Option kann jedoch auch zu einer Verlangsamung des Browsers führen, weil sie zum wiederholten Abrufen von Inhalten führt. Bei sehr langsamen Verbindungen können Probleme mit der Systemleistung auftreten. Alternativ können Sie Regeln für die Zwischenspeicherung festlegen, die es gestatten, dass bestimmte Inhalte wie Bilder, die eine bestimmte Größenbeschränkung nicht überschreiten, zwischengespeichert werden können.

Das IVE überprüft für jede Anforderung eines Benutzers die festgelegten Cacheregeln. Dabei können der Ursprungsserver, die angeforderte Datei und die Inhaltslänge entsprechend den Angaben des Ursprungsservers geprüft werden. Falls eine Regel zutrifft, wendet das IVE die festgelegte Richtlinie für das Zwischenspeichern an. Dabei kann es sich um eine von zwei Optionen für nicht zwischenspeicherungs-fähige Inhalte handeln:

- **Pragma: No-Cache (PNC)**

Bei entsprechender Einstellung fügt das Vermittlungsmodul der Antwort die Header `pragma:no-cache` und `cache-control:no-cache` hinzu. Darüber hinaus leitet das IVE die Cacheheader des Ursprungsservers (beispielsweise `age`, `date`, `etag`, `last-modified`, `expires`) nicht weiter.

- **Cache-Control: No-Store (CCNS)**

Wenn der Administrator CCNS auswählt, entfernt das Vermittlungsmodul die Cache-Control-Header des Ursprungsservers und fügt stattdessen einen Antwortheader vom Typ „`cache-control:no-store`“ hinzu, falls die vom Browser gesendete „`user-agent`“-Zeichenfolge das Element `msie` oder `windows-media-player` enthält.

Bei anderen Benutzer-Agenten fügt das IVE die Antwortheader PNC und CCNS hinzu und leitet die Cacheheader des Ursprungsservers nicht weiter. Wenn Sie festlegen, dass Inhalte *nicht* als nicht zwischenspeicherungs-fähig markiert werden, indem Sie beispielsweise die Richtlinien des Ursprungsservers nicht ändern, fügt das IVE nicht den Antwortheader `pragma:no-cache` oder `cache-control:no-store` hinzu, sondern leitet die Cacheheader des Ursprungsservers weiter.

Falls keine der festgelegten Regeln zutrifft, überprüft das IVE die vom Vermittlungsmodul verwendeten hartcodierten Regeln:

- **Zwischenspeicherung zulassen**

Das IVE fügt den Answerheader `pragma:no-cache` oder `cache-control:no-store` nicht hinzu und leitet die Cacheheader des Ursprungsservers weiter.

- **Zwischenspeicherung nur für Bilder unter einer bestimmten Größe zulassen**

Das IVE überprüft den „content-type“-Header des Ursprungsservers, der mit „image/“ beginnen muss, sowie den content-length-Header, der eine kleinere Größe als die angegebene Maximalgröße angeben. Falls das IVE feststellt, dass sich eine Anforderung auf ein Bild mit der richtigen Größe bezieht, fügt es den Answerheader `pragma:no-cache` oder `cache-control:no-store` nicht hinzu und leitet die Cacheheader des Ursprungsservers weiter. Andernfalls behandelt das IVE die Anforderung wie bei deaktivierter Zwischenspeicherung.

- **Zwischenspeicherung deaktivieren**

Das IVE leitet die Cacheheader vom Ursprungsserver nicht weiter. Falls das IVE im „user-agent“-Header das Element `msie` oder `windows-media-player` erkennt und sich die Anforderung auf eine Mediendatei bezieht, sendet das IVE den Answerheader `cache` oder `cache-control:no-store` nicht.

Beispiel:

```
(wenn in „content type“ das Element „audio/x-pn-realaudio“ steht ODER
wenn „content type“ mit „video/“ beginnt ODER
wenn „content type“ mit „audio/“ beginnt ODER
wenn „content type“ gleich „application/octet-stream“ ist und die
Dateierweiterung mit „rm“ oder „ram“ beginnt
)
```

In diesen Fällen entfernt das IVE den „cache-control“-Header des Ursprungsservers. Der Inhalt kann zwischengespeichert werden. Durch dieses Verhalten können Mediendateien ordnungsgemäß funktionieren.

Wenn das IVE im „user-agent“-Header das Element `msie` oder `windows-media-player` erkennt und sich die Anforderung auf bestimmte Arten von Dateien bezieht, sendet das IVE nicht den Header `pragma:no-cache`, sondern den Header `cache-control:no-store`, und entfernt den „cache-control“-Header des Ursprungsservers. Dieses Verhalten trifft auf die folgenden Fälle zu:

- Für Flash-Dateien, XLS-, PPS- und PPT-Dateien
- Wenn es sich bei „content-type“ um application/, text/rtf, text/xml oder model/ handelt
- Wenn der Ursprungsserver einen „content-disposition“-Header sendet

Andernfalls fügt das IVE, sofern die Regel zur Deaktivierung der Zwischenspeicherung angewendet wird, den Antwortheader pragma:no-cache oder cache-control:no-store hinzu.

---

**Hinweis:** ICA-Dateien von Citrix und QuickPlace-Dateien werden anders behandelt. ICA-Dateien von Citrix sind immer zwischenspeicherungsfähig und erhalten auch den Header „cache-control:private“. QuickPlace-Dateien, die keiner festgelegten Regel (die Vorrang hat) entsprechen, erhalten die Header CCNS und „cache-control:private“.

---

## Browserunterstützung

Bei den Cachesteuerungsdirektiven handelt es sich um W3C-Standards, die von allen kompatiblen Browsern unterstützt werden. In der folgenden Liste der von IVE unterstützten Browser werden die Header zur Cachesteuerung berücksichtigt:

- Win2k-IE5.5, SP2
- Win2k-IE 6.0
- Win98-Netscape 4.79
- Win98-IE5.5, SP2
- MacOS9.2-IE 5.1.5
- MacOSx-IE 5.2

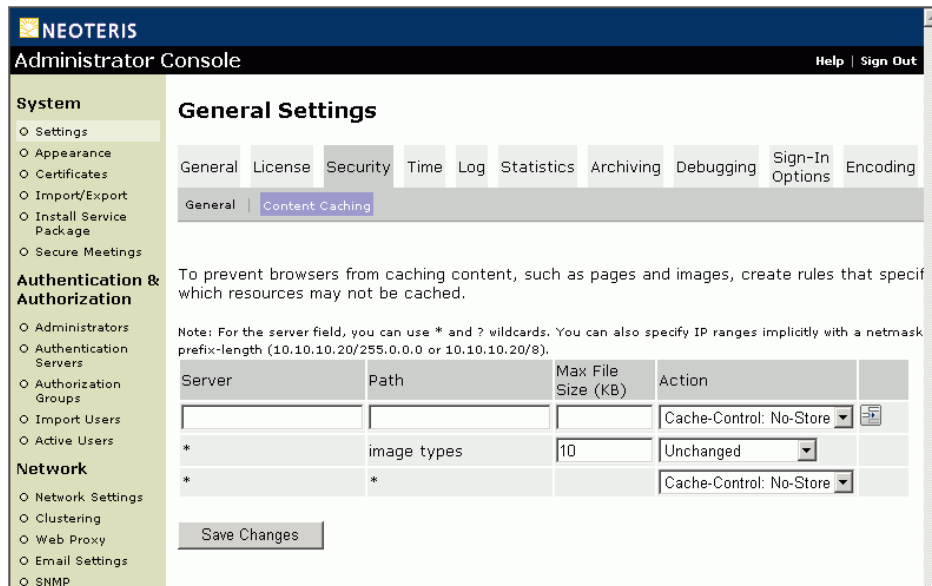


Abbildung 5: System > Settings > Security > Content Caching

## Registerkarte „Time“

### ☒ Einstellen der Systemzeit

Sie müssen die Serverzeit einstellen, damit die Systemereignisse und die Übertragung von Benutzerdateien genau aufgezeichnet werden.

#### So stellen Sie die Systemzeit ein

1. Klicken Sie in der Administratorkonsole auf die Registerkarte **System > Settings > Time**, um auf die Seite **Time** zuzugreifen. Oben auf der Seite werden das aktuelle Datum, die Uhrzeit und die Zeitzone des Geräts angezeigt.



2. Stellen Sie die Systemzeit mit Hilfe einer der folgenden Methoden ein:

- **Verwenden Sie einen NTP-Server.**

Klicken Sie nach der Frage „Use NTP server?“ auf **Yes**, geben Sie die IP-Adresse oder den Namen des Servers ein, legen Sie ein Aktualisierungsintervall fest, und klicken Sie auf **Save Changes**.

- **Stellen Sie die Systemzeit manuell ein.**

Geben Sie Werte für das Datum und die Uhrzeit ein, und klicken Sie auf **Save Changes**. Sie können auch auf **Get from Browser** klicken, damit Daten in die Felder **Date** und **Time** eingegeben werden.

3. Wählen Sie im Menü **Time Zone** eine Zeitzone aus, und klicken Sie auf **Save Changes**. Das IVE passt die Uhrzeit automatisch an die Sommerzeit an.

The screenshot shows the Neoteris Administrator Console interface. The left sidebar contains a menu with categories: System (Settings, Appearance, Certificates, Import/Export, Install Service Package, Secure Meetings), Authentication & Authorization (Administrators, Authentication Servers, Authorization Groups, Import Users, Active Users), and Network (Network Settings, Clustering, Web Proxy, Email Settings, SNMP). The main content area is titled 'General Settings' and has tabs for General, License, Security, Time (selected), Log, Statistics, Archiving, Debugging, Sign-In Options, and Encoding. The 'Time' tab displays the current system date and time: 'System Date: 7/21/2003' and 'System Time: 2:57:37 PM (GMT-08:00) Pacific Time (US & Canada); Tijuana'. Below this, there are three sections: 'Set time using NTP server' with radio buttons for 'Use NTP Server?' (Yes/No), a text field for 'NTP Server:', and a spinner for 'Update Interval:' (0 minutes); 'Set time zone' with a dropdown menu for 'Time Zone:' set to '(GMT-08:00) Pacific Time (US & Canada); Tijuana'; and 'Set time manually' with text fields for 'Date:' (mm/dd/yyyy) and 'Time:' (hh:mm:ss) with an AM/PM selector. Each section has a 'Save Changes' button. A 'Get from Browser' button is also present in the manual time setting section.

Abbildung 6: System > Settings > Time

## Unterregisterkarten „Log > View“ und „Log > Settings“

### ☒ Einstellen, Anzeigen, Löschen und Speichern des Systemprotokolls

Die Systemprotokolldatei ist eine auf dem Neoteris IVE-Server gespeicherte Textdatei, in der die folgenden Systemereignisse protokolliert werden:

- Änderungen des Administrators an den Benutzer-, System- und Netzwerkeinstellungen, beispielsweise Änderungen an Zeitüberschreitungen bei Sitzungen, an der Option zum Aktivieren bzw. Deaktivieren der URL-Navigation und an von Benutzern erstellten Lesezeichen sowie Geräte- und Serverinformationen
- Benutzeranmeldung und -abmeldung
- Zeitüberschreitungen bei Sitzungen, darunter Leerlaufzeiten und Überschreitungen der maximalen Sitzungslänge
- Systemfehler und -warnungen
- Dateianforderungen von Benutzern
- Webanforderungen
- Anzahl der gleichzeitig angemeldeten Benutzer im Intervall von jeweils einer Stunde (Anmeldung innerhalb der Stunde)
- Benachrichtigungen über einen Neustart des IVE-Dienstes (der IVE-Überwachungsprozess prüft in regelmäßigen Abständen den IVE-Server und startet ihn neu, falls das IVE nicht reagiert)
- Anforderungen zur Prüfung der Serververbindung

Auf der Seite **Log Settings** können Sie angeben, welche Ereignisse protokolliert werden, die maximale Dateigröße für das Systemprotokoll festlegen und einstellen, ob Ereignisse zusätzlich zur lokalen Protokollierung auch auf dem Syslog-Server protokolliert werden sollen. Auf der Seite **Log View** können Sie die festgelegte Anzahl an Ereignissen anzeigen, die Protokolldatei in einem Netzwerk speichern und das Protokoll löschen.

Wenn das Protokoll die maximal zulässige Dateigröße erreicht, werden die aktuellen Daten in die Datei `log.old` verschoben. Auf diese Weise stellt das System sicher, dass zumindest die maximale Dateigröße für die Daten beibehalten wird und dass Sie immer Zugriff auf die doppelte Menge an Daten haben und zwar in den aktuellen und in den alten Protokolldateien.

**Wichtig:** Vergewissern Sie sich, dass der Syslog-Server Nachrichten mit den folgenden Einstellungen akzeptiert: `facility = LOG_USER` und `level = LOG_INFO`.

Weitere Informationen zum Festlegen eines Archivierungsplans für das Systemprotokoll finden Sie unter „Planen der Archivierung von Systeminformationen“ auf Seite 24.

### **So legen Sie die Protokolleinstellungen fest**

1. Klicken Sie in der Administratorkonsole auf die Unterregisterkarte **System > Settings > Log > Settings**, um für das Systemprotokoll auf die Seite **Settings** zuzugreifen.
2. Legen Sie die maximale Dateigröße für die lokale Protokolldatei fest. (Die Grenze liegt bei 500 MB.) Im Systemprotokoll werden Daten bis zu der angegebenen Menge angezeigt.
3. Prüfen Sie, welche Ereignisse in der lokalen Protokolldatei erfasst werden sollen. Wenn diese Ereignisse auch in der syslog-Netzwerkdatei aufgezeichnet werden sollen, geben Sie den Namen oder die IP-Adresse des Syslog-Servers an.
4. Klicken Sie auf **Save Changes**. Die Änderungen werden sofort wirksam.

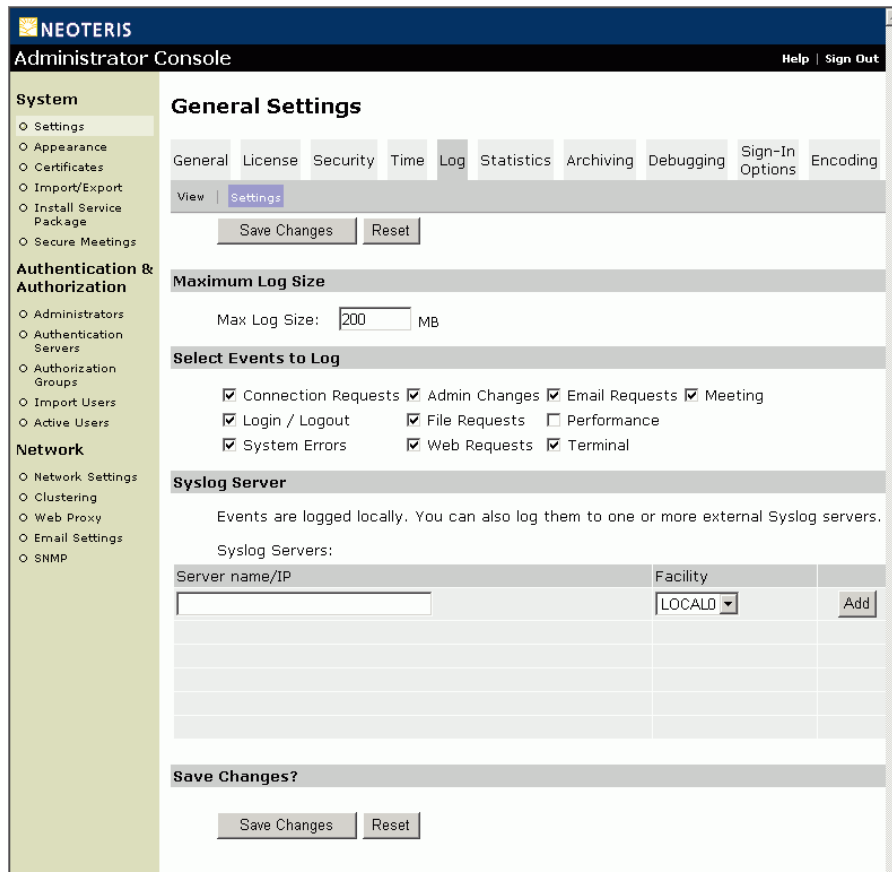


Abbildung 7: System > Settings > Log > Settings

**So zeigen Sie die Systemprotokolldatei an, speichern oder löschen sie**

1. Klicken Sie in der Administratorkonsole auf die Unterregisterkarte **System > Settings > Log > View**, um für das Systemprotokoll auf die Seite **View** zuzugreifen. Auf dieser Seite werden die neuesten Systemdaten des Tages angezeigt.

## 2. Führen Sie eine der folgenden Aufgaben durch:

- Zur Begrenzung der Anzahl an Ereignissen, die gleichzeitig angezeigt werden, geben Sie die gewünschte Anzahl der anzuzeigenden Nachrichten ein und klicken auf **Update**.
- Zur Speicherung der Protokolldatei klicken Sie auf **Save Log As**, wechseln zum gewünschten Netzwerkspeicherort, geben einen Dateinamen ein und klicken dann auf **Save**.
- Zum Löschen des lokalen Protokolls und der Datei log.o1d klicken Sie auf **Clear Log**.

---

**Hinweis:** Wenn Sie das lokale Protokoll löschen, wirkt sich dies nicht auf die vom Syslog-Server aufgezeichneten Ereignisse aus. Die nachfolgenden Ereignisse werden in einer neuen lokalen Protokolldatei aufgezeichnet.

---

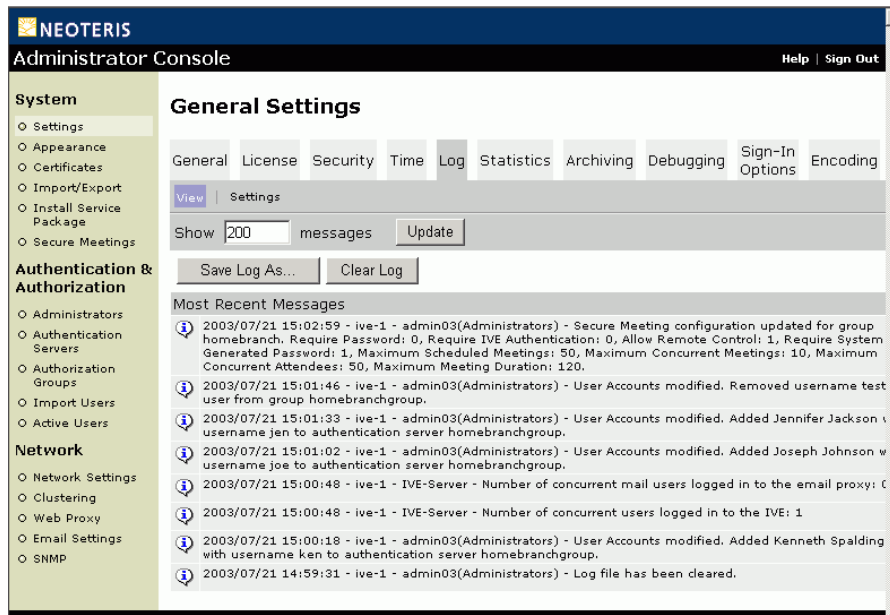


Abbildung 8: System > Settings > Log > View

## Registerkarte „Statistics“

### ☒ Anzeigen der Systemstatistik

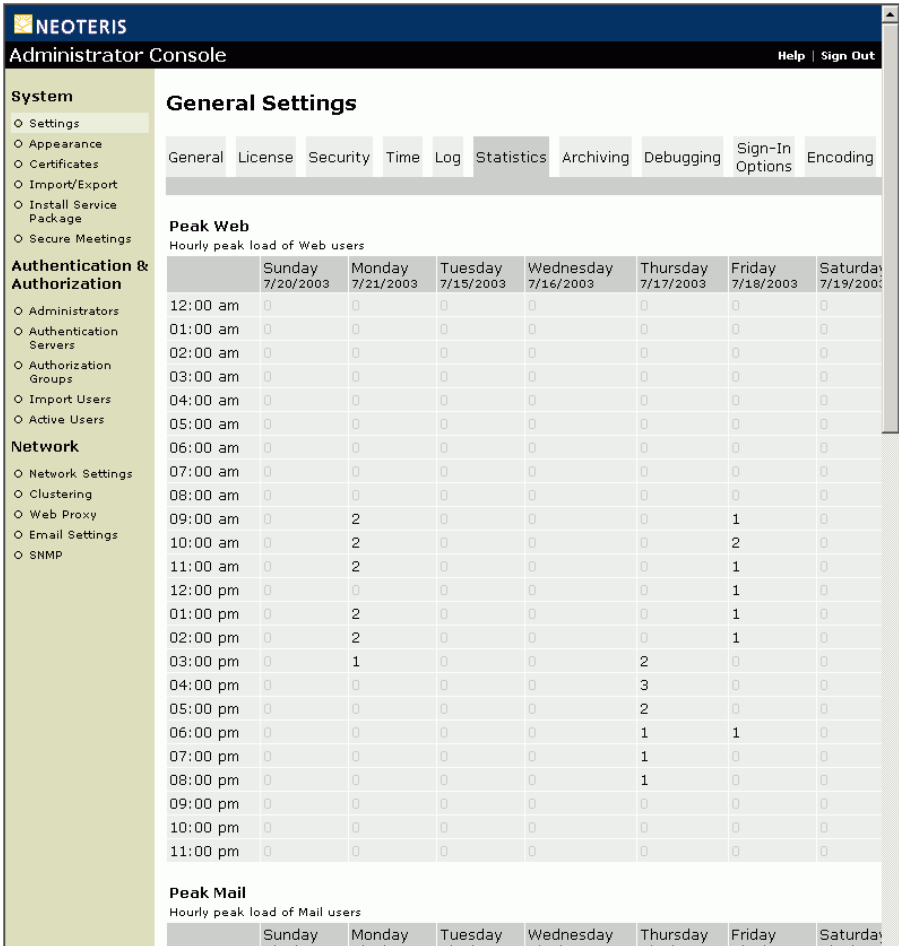
Das IVE protokolliert stündlich die folgenden Daten:

- Spitzenbelastung durch Webbenutzer
- Spitzenbelastung durch E-Mail-Benutzer
- Anzahl der URLs, auf die zugegriffen wird
- Anzahl der Dateien, auf die zugegriffen wird

Auf der Seite **Statistics** werden die Informationen für die letzten sieben Tage angezeigt. Diese Informationen werden einmal in der Woche und nach einer Aktualisierung in das Systemprotokoll geschrieben.

### So zeigen Sie die Systemstatistik an

1. Klicken Sie in der Administratorkonsole auf die Registerkarte **System > Settings > Statistics**, um auf die Seite **Statistics** zuzugreifen.
2. Führen Sie auf der Seite einen Bildlauf durch, um alle vier Datenkategorien anzuzeigen.



## Registerkarte „Archiving“

### ☒ Planen der Archivierung von Systeminformationen

Sie können festlegen, dass Systemprotokolldateien, Konfigurationsdateien und Benutzerkonten täglich oder wöchentlich archiviert werden. Das IVE archiviert die Dateien an den von Ihnen ausgewählten Tagen und Uhrzeiten über FTP auf dem angegebenen Server und in dem angegebenen Verzeichnis. Die Konfigurationsdateien und Benutzerkonten werden verschlüsselt, um eine sichere Übertragung über FTP und eine sichere Speicherung auf anderen Servern zu gewährleisten.

Der Name der Archivdateien enthält, wie nachfolgend dargestellt, das Datum und die Uhrzeit der Archivierung:

- Systemprotokolldateien: *NeoterisLog-Datum-Uhrzeit*
- Systemkonfigurationsdateien: *NeoterisConf-Datum-Uhrzeit*
- Benutzerkonten: *NeoterisUserAccounts-Datum-Uhrzeit*

### So legen Sie Archivierungsparameter fest

1. Klicken Sie in der Administratorkonsole auf die Registerkarte **System > Settings > Archiving**, um auf die Seite **Archiving** zuzugreifen.
2. Geben Sie unter **Archive Settings** den Zielserver, ein Verzeichnis und Ihre FTP-Anmeldeinformationen für diesen Server an. Schließen Sie keine Laufwerksangabe für das Zielverzeichnis ein, beispielsweise: *neoteris/log*.
  - Bei UNIX-Computern geben Sie abhängig vom Basisverzeichnis des Benutzers entweder einen absoluten oder einen relativen Pfad an.
  - Bei Windows-Computern geben Sie einen Pfad an, der relativ zum Ordner *ftproot* ist.
3. Für alle Arten von archivierten Daten geben Sie einen Archivierungsplan an. Für Systemprotokolldateien können Sie auswählen, ob die Protokolldatei nach ihrer Archivierung gelöscht werden soll.
4. Klicken Sie auf **Save Changes**.



NEOTERIS

Administrator Console

Help | Sign Out

System

- Settings
- Appearance
- Certificates
- Import/Export
- Install Service Package
- Secure Meetings

Authentication & Authorization

- Administrators
- Authentication Servers
- Authorization Groups
- Import Users
- Active Users

Network

- Network Settings
- Clustering
- Web Proxy
- Email Settings
- SNMP

General Settings

GeneralLicenseSecurityTimeLogStatisticsArchivingDebuggingSign-In OptionsEncoding

You can schedule automatic archiving of log data, system configuration, and user accounts. To do so, specify an FTP accessible location for the data, an FTP account to use, and the specific schedule for each type of archived data.

Archive Settings

Archive Server:Name or IP address

Destination Directory:

FTP Username:

FTP Password:

Archive Schedule

☐ Archive log data

Sun Mon Tue Wed Thu Fri Sat

☐☐☐☐☐☐☐

Time:  AM

☐ Clear log after archiving

☐ Archive system configuration

Sun Mon Tue Wed Thu Fri Sat

☐☐☐☐☐☐☐

Time:  AM

You can password-protect the archived system configuration files. If you do so, the password will need to be provided to import them.

Password for configuration file:

☐ Archive user accounts

Sun Mon Tue Wed Thu Fri Sat

☐☐☐☐☐☐☐

Time:  AM

You can password-protect the archived user configuration files. If you do so, the password will need to be provided to import them.

Password for configuration file:

Save Changes?

Save Changes

Abbildung 10: System > Settings > Archiving

## Debugging > Unterregisterkarte „Trace“

### ☒ Aufzeichnen einer Ablaufverfolgungsdatei zu Debuggingzwecken

Auf dieser Registerkarte können Sie eine Ablaufverfolgungsdatei aufzeichnen, in der die Aktionen eines Benutzers beim Navigieren zu einer Website aufgeführt werden, die nicht ordnungsgemäß angezeigt wird. Wenn Sie diese Option verwenden, erzwingt das IVE eine erneute Anmeldung des angegebenen Benutzers und beginnt dann mit der Aufzeichnung sämtlicher Benutzeraktionen. Beachten Sie, dass das IVE die Benutzer über die Aufzeichnung der Benutzeraktionen benachrichtigt.

#### So zeichnen Sie eine Ablaufverfolgungsdatei auf

1. Klicken Sie in der Administratorkonsole auf die Registerkarte **System > Settings > Debugging > Trace**.
2. Geben Sie den Benutzernamen des Benutzers ein, und klicken Sie auf **Start Recording**.
3. Weisen Sie den Benutzer an, zu der problematischen Website zu navigieren.
4. Klicken Sie auf **Stop Recording**.
5. Klicken Sie auf **Download**, um die Datei auf einen Netzwerkcomputer herunterzuladen. Entfernen Sie alle vertraulichen Daten mithilfe eines Text-Editors.
6. Senden Sie die Datei zur Überprüfung per E-Mail an die folgende Adresse: [help@support.neoteris.com](mailto:help@support.neoteris.com).

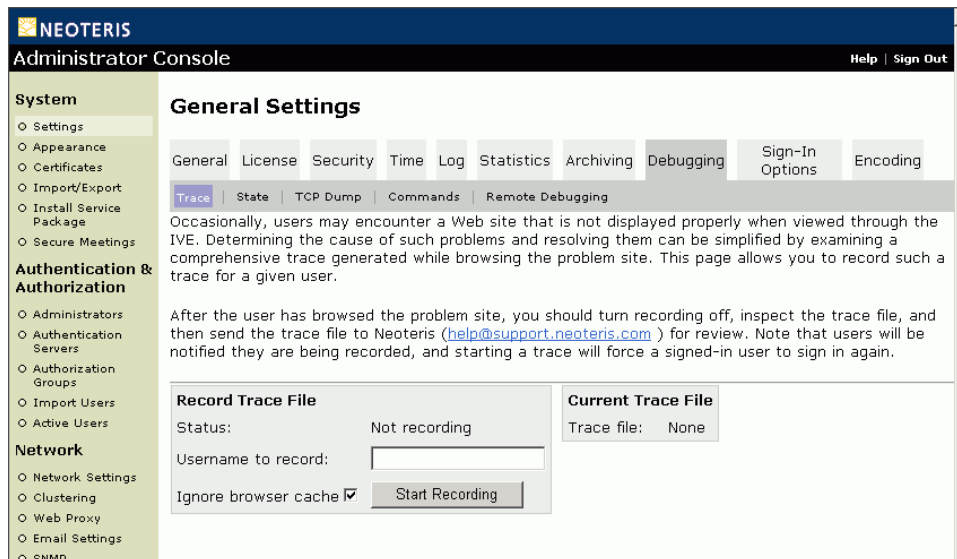


Abbildung 11: System &gt; Settings &gt; Debugging &gt; Trace

## Debugging > Unterregisterkarte „State“

### ☒ Erstellen eines Snapshots des IVE-Systemstatus.

Erstellen Sie auf dieser Registerkarte einen Snapshot des IVE-Systemstatus. Wenn Sie diese Option verwenden, führt das IVE verschiedene Dienstprogramme aus, um Details zum IVE-Systemstatus zu erfassen, beispielsweise zum belegten Speicherplatz, zur Auslagerungsleistung, zur Anzahl der ausgeführten Prozesse, zur Systembetriebszeit, zur Anzahl der geöffneten Dateibeschreibungen und zu den verwendeten Ports. Das IVE speichert bis zu zehn Snapshots, die in einer verschlüsselten „Dumpdatei“ bzw. Sicherungsdatei abgelegt werden. Diese können Sie auf einen Netzwerkcomputer herunterladen und dann per E-Mail an den Neoteris Support senden.

### So erstellen Sie einen Snapshot des IVE-Systemstatus

1. Klicken Sie in der Administratorkonsole auf die Registerkarte **System > Settings > Debugging > State**.
2. Klicken Sie auf **Make Snapshot**.

3. Wenn das IVE das Erstellen des Snapshots beendet hat, klicken Sie auf **Download**, um die Datei auf einen Netzwerkcomputer herunterzuladen.
4. Senden Sie die Datei zur Überprüfung per E-Mail an die folgende Adresse: [help@support.neoteris.com](mailto:help@support.neoteris.com).

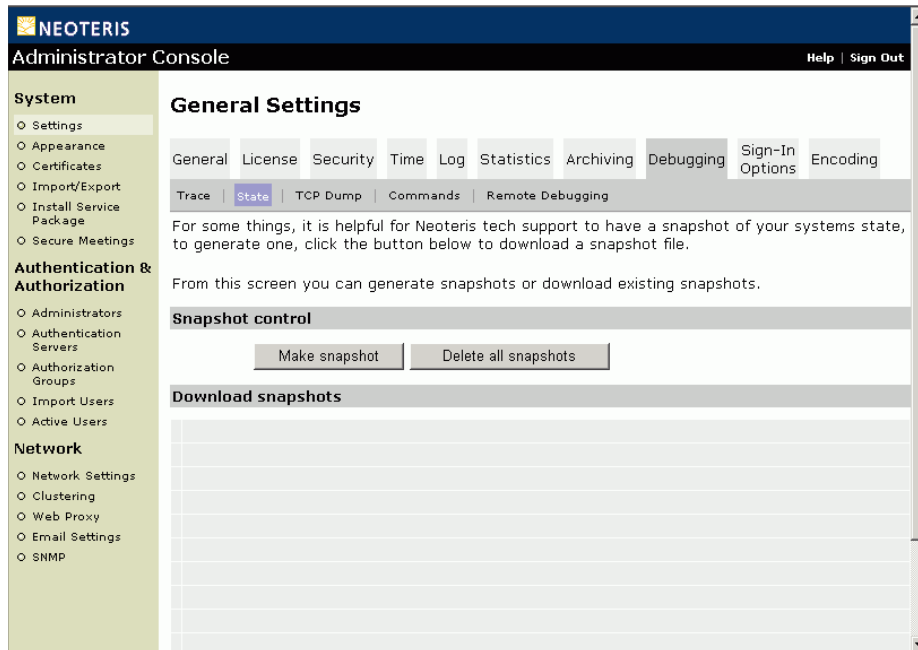


Abbildung 12: System > Settings > Debugging > State

## Debugging > Unterregisterkarte „TCP Dump“

### ☒ Abhören von Netzwerkpaketheadern mit einem Sniffer-Programm

Auf dieser Registerkarte können Sie Netzwerkpaketheader mit einem Sniffer-Programm abhören und die Ergebnisse in einer verschlüsselten „Dumpdatei“ bzw. Sicherungsdatei speichern. Diese können Sie auf einen Netzwerkcomputer herunterladen und dann per E-Mail an den Neoteris Support senden.

## So hören Sie Netzwerkpaketheader mit einem Sniffer-Programm ab

1. Klicken Sie in der Administratorkonsole auf die Registerkarte **System > Settings > Debugging > TCP Dump**.
2. Wählen Sie den IVE-Port aus, an dem die Netzwerkpaketheader mit einem Sniffer-Programm abgehört werden sollen. Deaktivieren Sie den **promiscuous**-Modus, so dass nur Pakete abgehört werden, die für das IVE bestimmt sind.
3. Klicken Sie auf **Stop Sniffing**, um das Abhören zu beenden und eine verschlüsselte Datei zu erstellen.
4. Klicken Sie auf **Download**, um die Datei auf einen Netzwerkcomputer herunterzuladen.
5. Senden Sie die Datei zur Überprüfung per E-Mail an die folgende Adresse: [help@support.neoteris.com](mailto:help@support.neoteris.com).

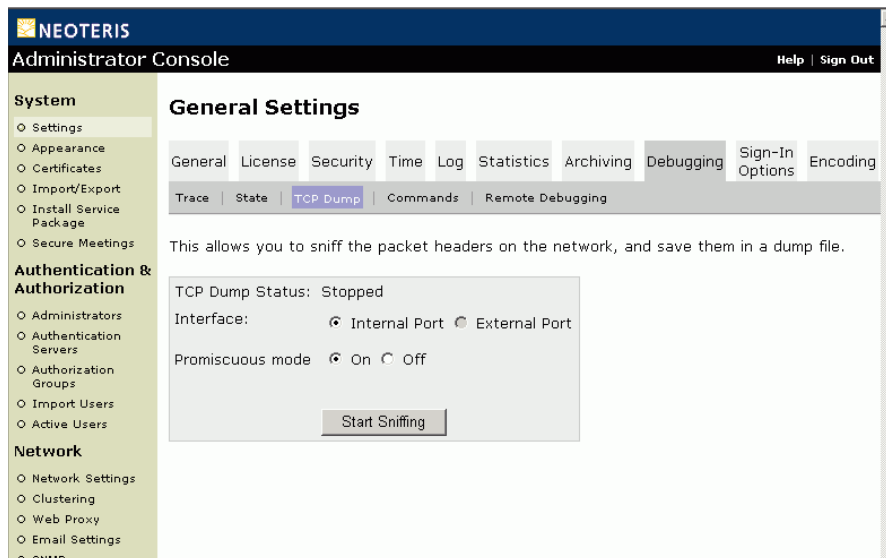


Abbildung 13: System > Settings > Debugging > TCP Dump

## Debugging > Unterregisterkarte „Commands“

### ☑ Ausführen eines ARP-, ping-, traceroute- oder nslookup-Befehls

Auf dieser Registerkarte können Sie UNIX-Befehle ausführen, um die IVE-Netzwerkverbindung zu testen.

#### So führen Sie einen UNIX-Befehl aus, um die IVE-Netzwerkverbindung zu testen

1. Klicken Sie in der Administratorkonsole auf die Registerkarte **System > Settings > Debugging > Commands**.
2. Wählen Sie im Menü **Command** den Befehl aus, der ausgeführt werden soll.
3. Geben Sie im Feld **Target Server** die IP-Adresse des Zielserver ein.
4. Klicken Sie zur Ausführung des Befehls auf **OK**.

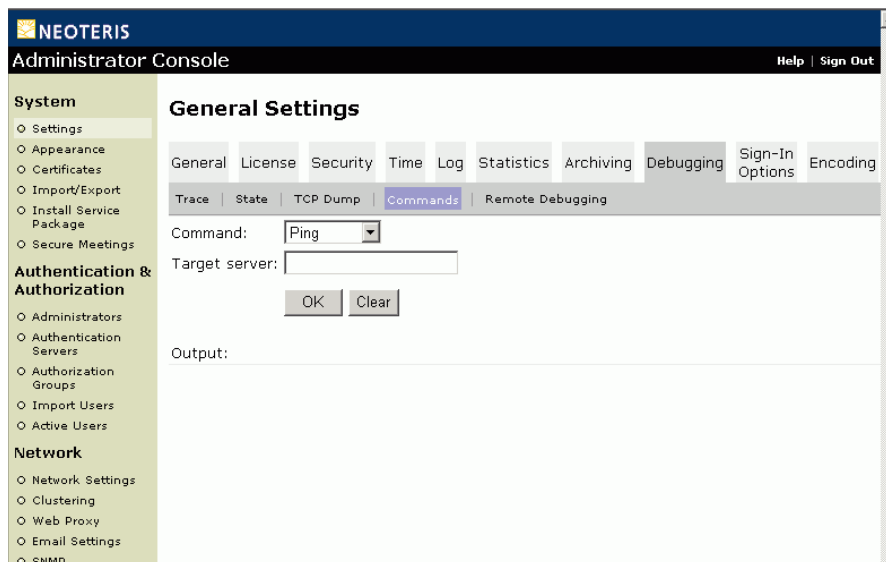


Abbildung 14: System > Settings > Debugging > Commands

## Debugging > Unterregisterkarte „Remote Debugging“

### ☒ Aktivieren von Remotedebugging für den Neoteris-Support

Auf dieser Registerkarte können Sie es dem Neoteris Support-Team ermöglichen, auf Ihrem Produktions-IVE Debuggingtools auszuführen. Zur Aktivierung dieser Option müssen Sie mit dem Neoteris-Support zusammenarbeiten, um einen Debuggingcode sowie einen Host zu erhalten, mit dem das IVE die Verbindung herstellt.

#### So aktivieren Sie Remotedebugging

1. Wenden Sie sich an den Neoteris Support, um die Bedingungen für eine Remotedebuggingsitzung festzulegen.
2. Klicken Sie in der Administratorkonsole auf die Registerkarte **System > Settings > Debugging > Remote Debugging**.
3. Geben Sie den Debuggingcode ein, der vom Neoteris-Support zur Verfügung gestellt wurde.
4. Geben Sie den Hostnamen ein, der vom Neoteris-Support zur Verfügung gestellt wurde.
5. Klicken Sie auf **Enable Debugging**, so dass das Neoteris-Support-Team auf das IVE zugreifen kann.
6. Teilen Sie dem Neoteris-Support mit, dass auf Ihr IVE zugegriffen werden kann.
7. Klicken Sie auf **Disable Debugging**, wenn der Neoteris-Support Ihnen mitteilt, dass die Remotedebuggingsitzung beendet ist.

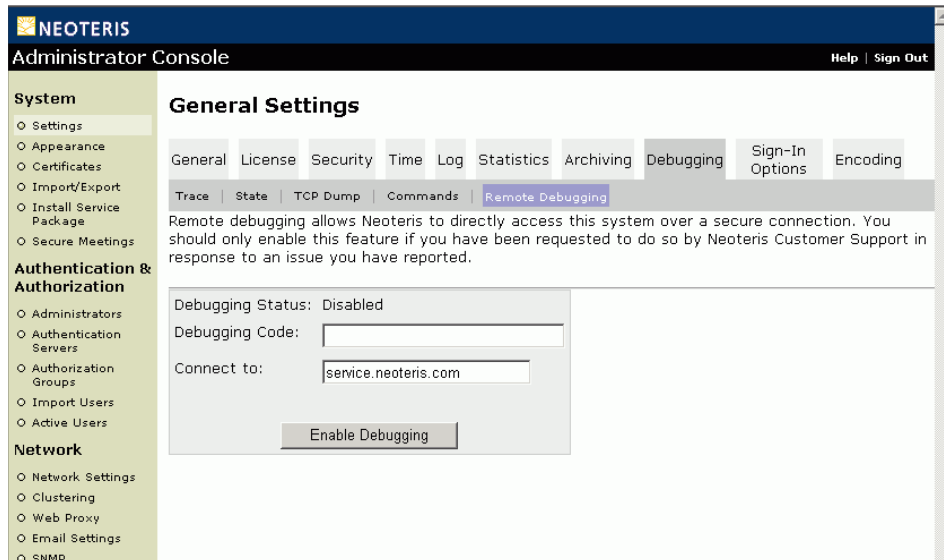


Abbildung 15: System > Settings > Debugging > Remote Debugging

## Sign-in Options > Unterregisterkarte „Restrictions“

### ☑ Festlegen systemweiter Anmeldeeinschränkungen

Auf dieser Registerkarte können Sie für den Zugriff auf einen IVE zwischen allen aktivierten Authentifizierungsservern und den zugeordneten Benutzern sowie Benutzern der Administratorengruppe umschalten.

#### So schränken Sie den Zugriff auf das IVE auf die Administratorengruppe ein

1. Klicken Sie in der Administratorkonsole auf die Registerkarte **System > Settings > Sign-In Options > Restrictions**.
2. Wählen Sie **Administrators Only**, und klicken Sie auf **Save Changes**.



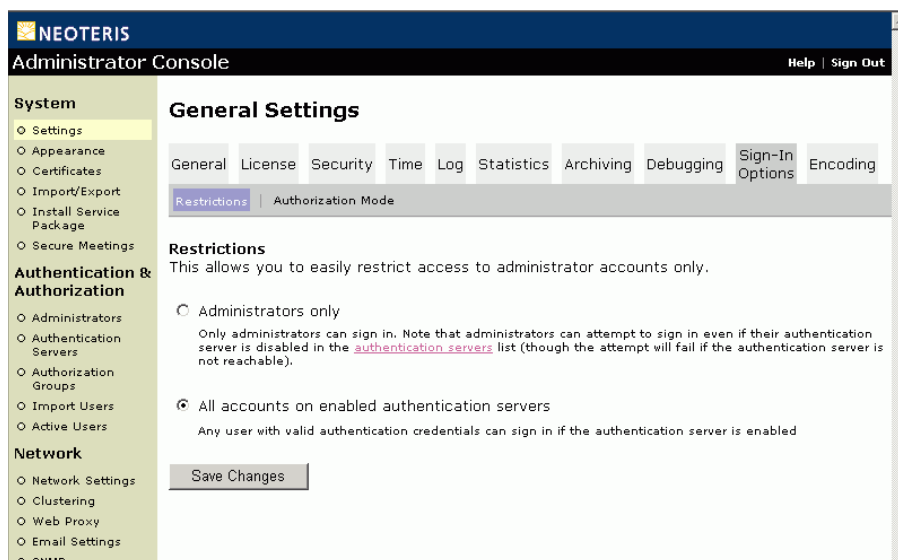


Abbildung 16: System > Settings > Sign-In Options > Restrictions

## Sign-In Options > Unterregisterkarte „Authorization Mode“

### ☒ Festlegen systemweiter Anmeldeoptionen

Auf dieser Registerkarte können Sie das Anmeldeverhalten von Benutzern steuern.

#### So legen Sie systemweite Anmeldeoptionen fest

1. Klicken Sie in der Administratorkonsole auf die Registerkarte **System > Settings > Sign-In Options > Authorization Mode**.
2. Wählen Sie die entsprechenden Optionen aus, und klicken Sie dann auf **Save Changes**. Folgende Optionen stehen zur Verfügung:
  - **User selects authentication server from a list**  
Das IVE zeigt alle aktivierten Authentifizierungsserver an, die auf der Anmeldeseite in der Dropdownliste **Server** enthalten sind.
  - **User types authentication server name**  
Das IVE zeigt ein Textfeld an, in das der Benutzer den Authentifizierungsserver eingeben muss, an dem er sich anmelden möchte.

- **User is assigned to the first matching group**  
Für die IVE-Sitzung des Benutzers wird die erste Gruppe verwendet, der das IVE den Benutzer zuordnet.
- **User selects group from among all matching groups**  
Das IVE zeigt eine Seite an, auf der sämtliche Gruppen aufgeführt werden, denen ein Benutzer zugeordnet ist, so dass der Benutzer auswählen kann, welcher Gruppe er für die IVE-Sitzung beitreten möchte.
- **Enable 2.x authorization mode**  
Durch diese Option werden die in den 2.x-Versionen des IVE verwendeten Authentifizierungs- und Autorisierungsverfahren aktiviert.

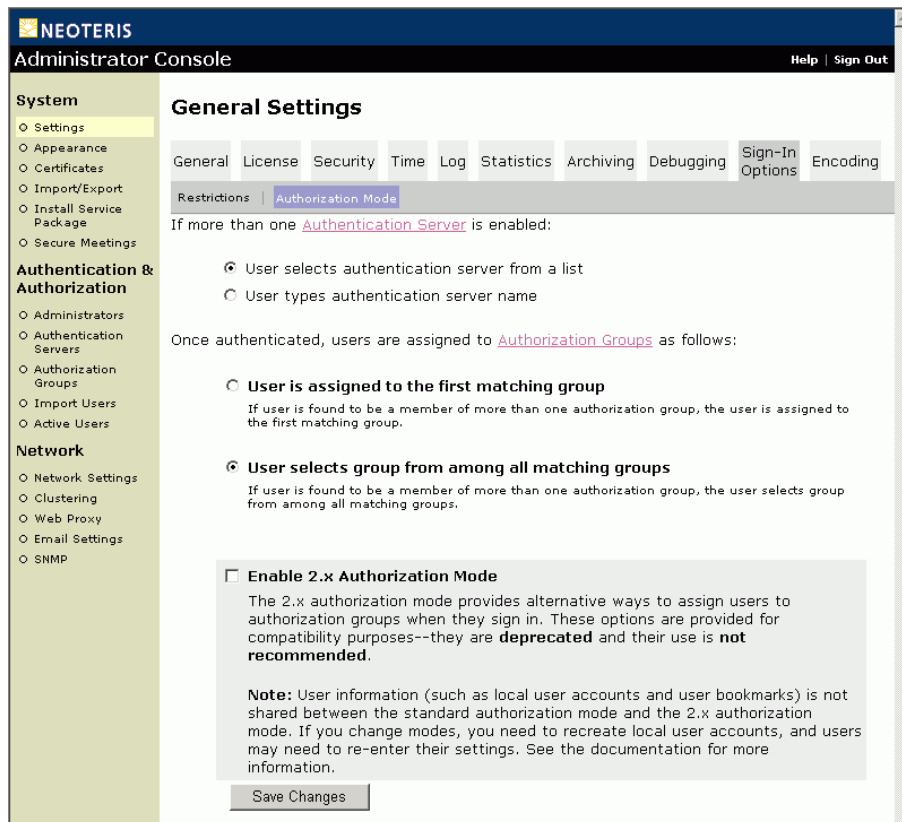


Abbildung 17: System > Settings > Sign-In Options > Authorization Mode

## Registerkarte „Encoding“

### ☑ Festlegen der Codierung für die Internationalisierung

Auf dieser Registerkarte können Sie festlegen, wie das IVE die Daten bei der Interaktion mit Dateiservern codiert.

#### So legen Sie fest, wie der IVE-Datenverkehr codiert wird

1. Klicken Sie in der Administratorkonsole auf die Registerkarte **System > Settings > Encoding**.
2. Wählen Sie die entsprechende Option aus, und klicken Sie dann auf **Save Changes**.

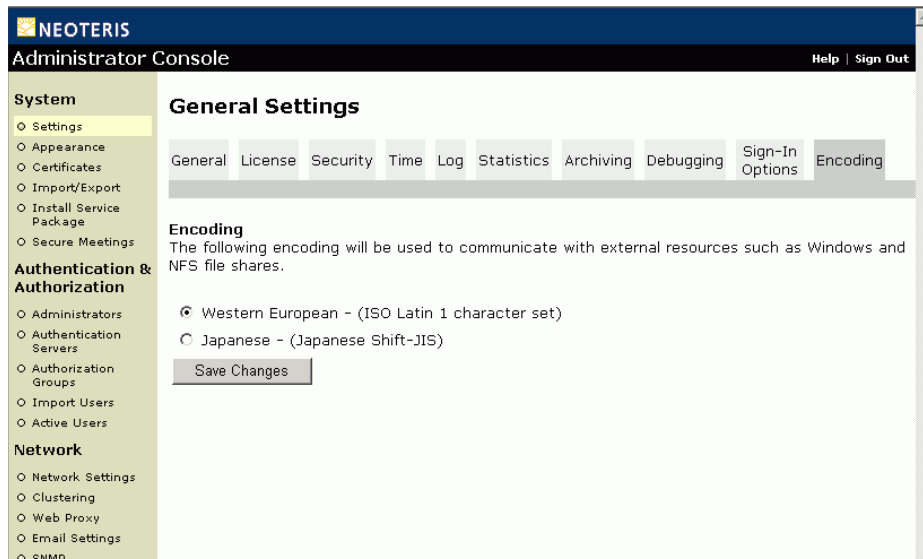


Abbildung 18: System > Settings > Encoding

## System > Menü „Appearance“

Auf den Registerkarten des Menüs **Appearance** können Sie die Anmeldeseite für Administratoren und Benutzer, die IVE-Startseite und die Administratorkonsole anpassen, indem Sie folgende Aktionen ausführen:

- Ändern des Logos und der Farbe des Seitenkopfs
- Ändern des Symbols der Symbolleiste zum Durchsuchen
- Personalisieren der Begrüßungsnachricht
- Ändern der Begrüßung des Benutzers und der Anweisungen auf der Anmeldeseite
- Ändern der Anweisungen, die angezeigt werden, wenn ein Zertifikat fehlt oder ungültig ist
- Hinzufügen einer Hilfeschaftfläche zu der Anmeldeseite, die mit einer benutzerdefinierten HTML-Datei verknüpft ist

### Registerkarte „General“

#### ☒ Anpassen der Darstellung des IVE

Wenn sich ein Benutzer am Neoteris IVE anmeldet, wird die IVE-Startseite mit Ihren benutzerdefinierten Einstellungen angezeigt. Auf der Neoteris IVE-Symbolleiste zum Durchsuchen (**Abbildung 19**) wird außerdem auf jeder Webseite, zu der ein Benutzer wechselt, das von Ihnen erstellte benutzerdefinierte Symbol angezeigt. Wenn der Benutzer auf dieses Symbol klickt, gelangt er über eine Verknüpfung zurück zur IVE-Startseite.

The logo image you  
specify appears here



**Abbildung 19: IVE-Symbolleiste zum Durchsuchen**

Sie können benutzerdefinierte Hilfeinformationen für die Benutzer bereitstellen. Konfigurieren Sie einfach das IVE zur Anzeige einer Hilfeschnittfläche auf der IVE-Anmeldeseite, und legen Sie eine HTML-Datei fest, die beim Klicken auf die Hilfeschnittfläche angezeigt werden soll.



Abbildung 20: Neoteris IVE-Anmeldeseite mit Hilfeschnittfläche

### So passen Sie die Darstellung des IVE an

1. Klicken Sie in der Administratorkonsole auf die Registerkarte **System > Appearance > General**, um auf die Seite **General** zuzugreifen.
2. Legen Sie im Abschnitt **Header** eine benutzerdefinierte Logobilddatei und eine andere Farbe für den Seitenkopf fest.
3. Legen Sie im Abschnitt **Browsing Toolbar** ein benutzerdefiniertes Symbol für die IVE-Symbolleiste zum Durchsuchen fest. Die empfohlene Größe für das Symbol beträgt maximal 24 Quadratpixel bzw. ist kleiner als 6 KB. Sie können auch festlegen, dass die Symbolleiste nicht angezeigt wird.
4. Zur Personalisierung der Begrüßungsnachricht, die auf der Seite **Bookmarks** des IVE angezeigt wird, wählen Sie **Personalize welcome message in the Bookmarks page**. Bei Auswahl dieser Option wird in der Begrüßungsnachricht der vollständige Name des Benutzers (sofern verfügbar) oder der Benutzername angezeigt.
5. Klicken Sie auf **Save Changes**.

## Registerkarte „Sign-in Page“

### ☒ Anpassen der IVE-Anmeldeseite

#### So passen Sie die IVE-Endbenutzeroberfläche an

1. Klicken Sie in der Administratorkonsole auf die Registerkarte **System > Appearance > Sign-in**, um auf die Seite **Sign-in** zuzugreifen.
2. Ändern Sie in den Abschnitten **Custom Text** und **Custom Error Messages** den für die verschiedenen Fenstertitel verwendeten Standardtext nach Bedarf.
3. Um Benutzern benutzerdefinierte Hilfeinformationen oder zusätzliche Anweisungen bereitzustellen, wählen Sie **Help Button**, und legen Sie eine HTML-Datei fest, die in das Neoteris IVE hochgeladen werden soll. Beachten Sie, dass im IVE keine Bilder und anderen Inhalte angezeigt werden, auf die auf dieser HTML-Seite verwiesen wird.
4. Klicken Sie auf **Save Changes**. Die Änderungen werden sofort wirksam, doch möglicherweise muss bei den aktuellen Browsersitzungen von Benutzern eine Aktualisierung durchgeführt werden, damit die Änderungen angezeigt werden.

---

**Hinweis:** Klicken Sie auf **Restore Factory Defaults**, um die Darstellung der Anmeldeseite, der IVE-Startseite für Benutzer und der Administratorkonsole zurückzusetzen.

---

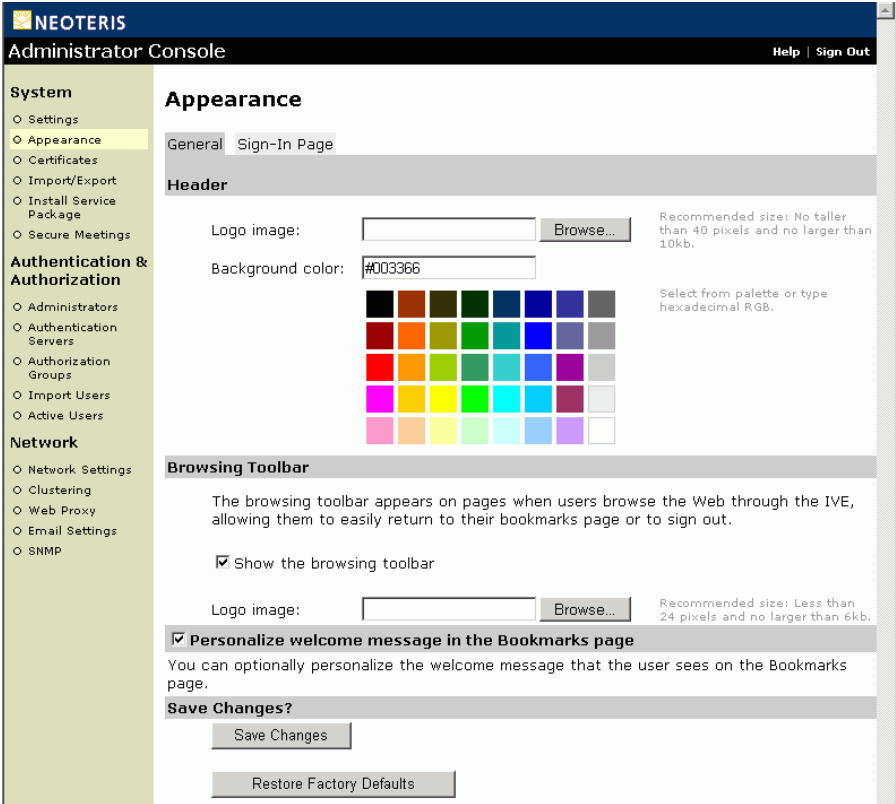


Abbildung 21: System > Appearance > General

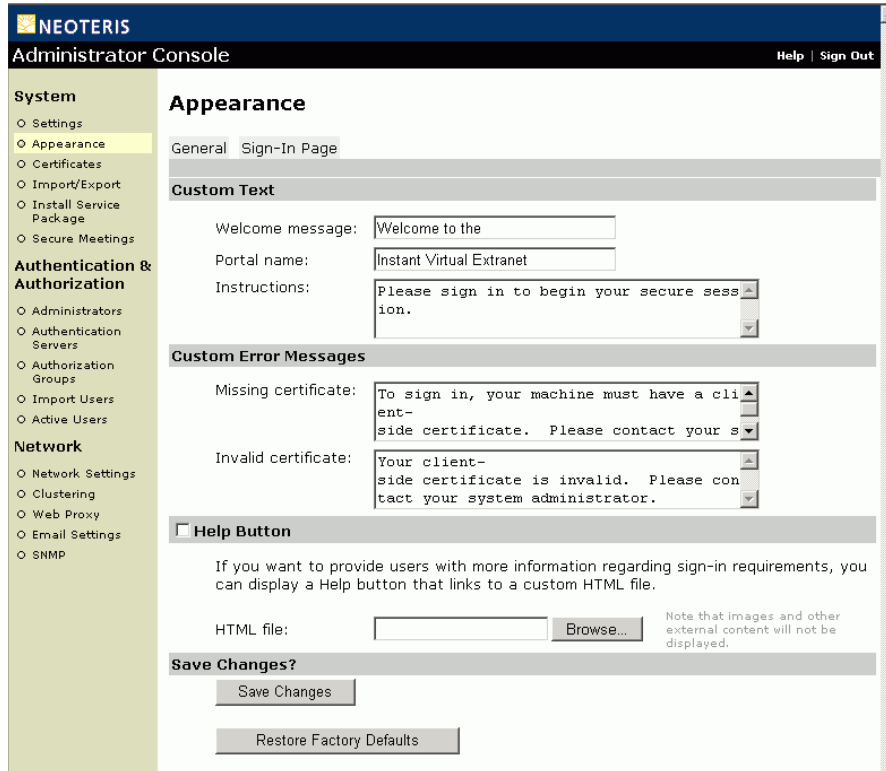


Abbildung 22: System > Appearance > Sign-In Page



## System > Menü „Certificates“

Auf den Registerkarten des Menüs **Certificates** können Sie die folgenden Aufgaben durchführen:

- Importieren eines bestehenden Serverzertifikats und eines privaten Schlüssels (43)
- Importieren eines erneuerten Serverzertifikats, für das der bestehende privater Schlüssel verwendet wird (45)
- Erstellen einer Zertifikatssignaturanforderung für ein neues Serverzertifikat (47)
- Importieren eines signierten Serverzertifikats, das anhand einer Zertifikatssignaturanforderung erstellt wurde (50)
- Importieren eines Stammzertifikats zur Überprüfung eines clientseitigen Zertifikats (52)
- Importieren eines Codesignaturzertifikats (55)

Ein digitales Zertifikat ist eine verschlüsselte elektronische Datei, in der die Anmeldeinformationen eines Webservers oder Benutzers für Client-Server-Transaktionen festgelegt werden. Der Neoteris IVE-Server verwendet ein temporäres, selbst signiertes digitales Zertifikat, das mit den bei der Initialisierung eingegebenen Daten lokal erstellt wird. Mit Hilfe dieses Zertifikats können die Benutzer sofort mit der Verwendung des IVE<sup>1</sup> beginnen.

Das IVE unterstützt X.509-Zertifikate in den folgenden Formaten:

- DER-, NET- oder PEM-verschlüsselt (Dateierweiterungen: .cer, .crt, .der, .net und .pem)
- PKCS #12 (Dateierweiterungen: .pfx und .p12)

Zum Erhalt eines digitalen Zertifikats für den Neoteris IVE-Server gibt es zwei Möglichkeiten:

- Ein bestehendes Serverzertifikat und einen privaten Schlüssel auf den Neoteris IVE-Server importieren. Zunächst müssen Sie das Serverzertifikat und den privaten Schlüssel vom vorhandenen Webserver exportieren. Anschließend importieren Sie diese Dateien über die IVE-Seite **Certificates > Server Certificate**. (Siehe Seite 43.)

---

1. Die Verschlüsselung für das während der Initialisierung erstellte selbst signierte Zertifikats ist zwar absolut sicher, doch für die Benutzer wird bei jeder Anmeldung am IVE eine Sicherheitswarnung angezeigt, da das Zertifikat nicht von einer Zertifizierungsstelle ausgestellt wird. Zu Produktionszwecken empfiehlt es sich, ein digitales Zertifikat von einer Zertifizierungsstelle zu beschaffen.

- Erstellen Sie eine Zertifikatssignaturanforderung (Certificate Signing Request, CSR), die an eine Zertifizierungsstelle gesendet wird (Seite 47). Wenn die Zertifizierungsstelle die signierte Datei zurücksendet, importieren Sie diese über die Seite **Certificates > Server Certificate** (Seite 50).

Sie können den Neoteris IVE-Server auch so konfigurieren, dass ein Benutzer ein gültiges clientseitiges Zertifikat angeben muss, damit er sich erfolgreich am System anmelden kann. Um festzulegen, dass ein Benutzer ein gültiges clientseitiges Zertifikat angeben muss, müssen Sie die folgenden Schritte ausführen:

- 1 Installieren Sie ein clientseitiges Zertifikat über den Browser des Benutzers. Hilfe dazu können Sie den Anweisungen zu dem Browser entnehmen. Bei weiteren Fragen in diesem Zusammenhang lesen Sie die Ihrer IVE-Version entsprechenden Versionshinweise.
- 2 Auf der Registerkarte **Certificates > CA Certificate** können Sie ein Stammzertifikat in das IVE importieren, das das clientseitige Zertifikat überprüft (Seite 52).
- 3 Auf der Unterregisterkarte **Authentication & Authorization > Authorization Groups > GroupName > Authentication > Certificate** legen Sie die entsprechenden Einstellungen für das clientseitige Zertifikat fest (Seite 142). Um das Setup zu vereinfachen, kann eine Gruppe die Einstellungen für das clientseitige Zertifikat erben, die Sie für die Benutzergruppe festlegen.

## Registerkarte „Server Certificate“

Wenn Ihr Unternehmen bereits ein digitales Serverzertifikat erworben hat, importieren Sie die Zertifikatsdatei und den entsprechenden Schlüssel über die Registerkarte **Server Certificate** in das IVE. Auf dieser Registerkarte können Sie auch ein auf dem bestehenden privaten Schlüssel basierendes erneuertes Zertifikat importieren oder ein Zertifikat importieren, das auf einer Zertifikatssignaturanforderung, die Sie bei einer Zertifizierungsstelle eingereicht haben.

Dieser Abschnitt umfasst folgende Aufgaben:

- Importieren eines bestehenden Serverzertifikats und eines privaten Schlüssels (43)
- Importieren eines erneuerten Serverzertifikats, für das der bestehende private Schlüssel verwendet wird (45)
- Erstellen einer Zertifikatssignaturanforderung für ein neues Serverzertifikat (47)
- Importieren eines signierten Serverzertifikats, das anhand einer Zertifikatssignaturanforderung erstellt wurde (50)

## ☑ Importieren eines bestehenden Serverzertifikats und eines privaten Schlüssels

Sie können Webserverzertifikate von Servern wie Apache, IIS, Sun ONE (früher iPlanet) oder Netscape erstellen und das Zertifikat dann in das IVE importieren. Zum Exportieren eines digitalen Serverzertifikats und eines Schlüssels befolgen Sie die zu dem Webserver vorhandenen Anweisungen zum Exportieren von Zertifikaten.

---

**Wichtig:** Das Zertifikat muss verschlüsselt sein, und Sie müssen das Kennwort mit dem Zertifikat exportieren.

---

### So importieren Sie ein bestehendes digitales Serverzertifikat und einen privaten Schlüssel

1. Klicken Sie in der Administratorkonsole auf die Registerkarte **System > Certificates > Server Certificate**.
2. Klicken Sie auf **Import / Renew**.
3. Wählen Sie das entsprechende Formular für den Import des Zertifikats aus:
  - Falls das Zertifikat und der Schlüssel in einer Datei enthalten sind, verwenden Sie das Formular **Certificate file includes private key**.
  - Handelt es sich bei dem Zertifikat und dem Schlüssel um separate Dateien, verwenden Sie das Formular **Certificate and private key are separate files**.
4. Wechseln Sie im entsprechenden Formular zu der Datei mit dem Zertifikat und dem Schlüssel. Geben Sie ggf. den Kennwortschlüssel ein.
5. Klicken Sie auf **Import**.

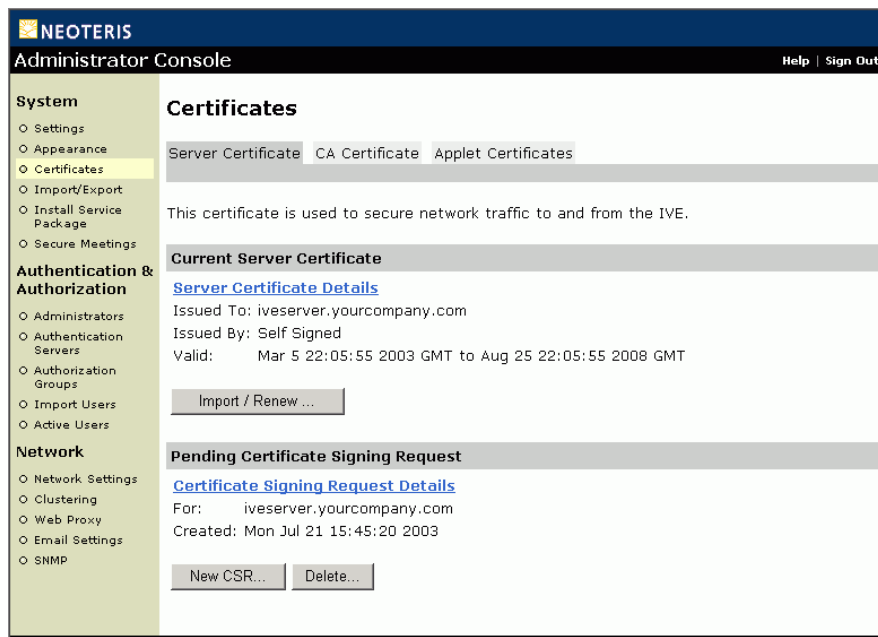


Abbildung 23: System > Certificates > Server Certificate

**NEOTERIS**  
Administrator Console Help | Sign Out

**System**  
○ Settings  
○ Appearance  
○ Certificates  
○ Import/Export  
○ Install Service Package  
○ Secure Meetings

**Authentication & Authorization**  
○ Administrators  
○ Authentication Servers  
○ Authorization Groups  
○ Import Users  
○ Active Users

**Network**  
○ Network Settings  
○ Clustering  
○ Web Proxy  
○ Email Settings  
○ SNMP

[Certificates >](#)  
**Import Certificate & Key**

Use one of the forms below to import an existing certificate and its corresponding private key. If the files are encrypted, you will also need to specify the password.

**Certificate file includes private key:**

Certificate File:  Browse...  
Password Key:   
Import

**Certificate and private key are separate files:**

Certificate File:  Browse...  
Private Key File:  Browse...  
Password Key:   
Import

**Renew the Certificate:**

Certificate File:  Browse...  
Renew

**Abbildung 24: System > Certificates > Server Certificate > Import / Renew ...**  
Verwenden Sie eines dieser Formulare, um ein Serverzertifikat und einen privaten Schlüssel zu importieren, die Sie bereits erworben haben.

## ☒ Importieren eines erneuerten Serverzertifikats, für das der bestehende privater Schlüssel verwendet wird

Sie können ein Serverzertifikat auf zwei Arten erneuern:

- **Bei einer Zertifizierungsstelle eine neue Zertifikatssignaturanforderung einreichen**

Dieser Vorgang zur Erneuerung eines Zertifikats ist sicherer, da die Zertifizierungsstelle ein neues Zertifikat und einen neuen privaten Schlüssel generiert und dabei die Gültigkeit des älteren privaten Schlüssels aufhebt. Zur Verwendung dieser Erneuerungsmethode müssen Sie zuerst über die Administrator-konsole eine Zertifikatssignaturanforderung erstellen. Weitere Informationen erhalten Sie unter „Erstellen einer Zertifikatssignaturanforderung für ein neues Serverzertifikat“ auf Seite 47.

- **Basierend auf der vorher bei der Zertifizierungsstelle eingereichten Zertifikatssignaturanforderung eine Erneuerung anfordern**

Dieser Vorgang zur Erneuerung eines Zertifikats ist weniger sicher, da die Zertifizierungsstelle ein Zertifikat generiert, für das der bestehende private Schlüssel verwendet wird.

---

**Wichtig:** Geben Sie bei der erneuten Anforderung eines Zertifikats dieselben Informationen an, die in der ursprünglichen Zertifikatssignaturanforderung verwendet wurden. Anhand dieser Informationen erstellt die Zertifizierungsstelle ein neues Zertifikat, das dem bestehenden Schlüssel entspricht.

---

**So importieren Sie ein erneuertes Serverzertifikat, für das ein bestehender privater Schlüssel verwendet wird**

1. Befolgen Sie die Anweisungen der Zertifizierungsstelle zur Erneuerung eines Zertifikats, das Sie zuvor dort erworben haben.

---

**Wichtig:** Vergewissern Sie sich, dass Sie dieselben Informationen angeben, die in der ursprünglichen Zertifikatssignaturanforderung verwendet wurden. Anhand dieser Informationen erstellt die Zertifizierungsstelle ein neues Zertifikat, das dem bestehenden Schlüssel entspricht.

---

2. Klicken Sie in der Administratorkonsole auf die Registerkarte **System > Certificates > Server Certificate**.
3. Klicken Sie auf **Import / Renew**.
4. Wechseln Sie im Formular **Renew the Certificate** zu der Datei mit dem erneuerten Zertifikat, und klicken Sie dann auf **Renew**.

**NEOTERIS**  
Administrator Console Help | Sign Out

**System**  
○ Settings  
○ Appearance  
○ Certificates  
○ Import/Export  
○ Install Service Package  
○ Secure Meetings

**Authentication & Authorization**  
○ Administrators  
○ Authentication Servers  
○ Authorization Groups  
○ Import Users  
○ Active Users

**Network**  
○ Network Settings  
○ Clustering  
○ Web Proxy  
○ Email Settings  
○ SNMP

[Certificates >](#)  
**Import Certificate & Key**

Use one of the forms below to import an existing certificate and its corresponding private key. If the files are encrypted, you will also need to specify the password.

**Certificate file includes private key:**

Certificate File:    
Password Key:

**Certificate and private key are separate files:**

Certificate File:    
Private Key File:    
Password Key:

**Renew the Certificate:**

Certificate File:

**Abbildung 25: System > Certificates > Server Certificate > Import / Renew ...**  
Wechseln Sie über das Formular **Renew the Certificate** zu dem erneuerten Zertifikat von der Zertifizierungsstelle.

## ☑ Erstellen einer Zertifikatssignaturanforderung für ein neues Serverzertifikat

Falls Ihr Unternehmen über kein digitales Zertifikat für die Webserver verfügt, können Sie über die Administratorkonsole eine Zertifikatssignaturanforderung erstellen und diese dann zur Verarbeitung an eine Zertifizierungsstelle senden. Wenn Sie über die Administratorkonsole eine Zertifikatssignaturanforderung erstellen, wird lokal ein privater Schlüssel erstellt, der der Zertifikatssignaturanforderung entspricht. Falls Sie die Zertifikatssignaturanforderung löschen, wird diese Datei ebenfalls gelöscht. Es ist dann nicht mehr möglich, ein über die Zertifikatssignaturanforderung erstelltes signiertes Zertifikat zu installieren.

---

**Wichtig:** Senden Sie nur jeweils eine Zertifikatssignaturanforderung an eine Zertifizierungsstelle. Andernfalls fallen u. U. doppelte Gebühren an.

---

### So erstellen Sie eine Zertifikatssignaturanforderung

1. Klicken Sie in der Administratorkonsole auf die Registerkarte **System > Certificates > Server Certificate**.
2. Klicken Sie unter **Pending Certificate Signing Request** auf **New CSR**.
3. Geben Sie die erforderlichen Informationen ein (**Abbildung 26** auf Seite 49), und klicken Sie auf **Create CSR**.
4. Befolgen Sie die Anweisungen auf dem Bildschirm (**Abbildung 27** auf Seite 50). Darin wird neben dem Sendeverfahren erläutert, welche Informationen an die Zertifizierungsstelle gesendet werden müssen. Wenn Sie von der Zertifizierungsstelle ein signiertes Zertifikat erhalten, importieren Sie die Zertifikatdatei. Befolgen Sie dabei die unter „Importieren eines signierten Serverzertifikats, das anhand einer Zertifikatssignaturanforderung erstellt wurde“ auf Seite 50 angegebenen Anweisungen.

---

**Hinweis:** Wenn Sie eine Zertifikatssignaturanforderung bei einer Zertifizierungsstelle einreichen, werden Sie u. U. dazu aufgefordert, entweder den Typ des Web-servers anzugeben, auf dem das Zertifikat erstellt wurde, oder den Typ des Web-servers, für den das Zertifikat bestimmt ist. Wählen Sie **apache\_modssl** (falls mehrere Optionen mit „apache\_modssl“ verfügbar sind, wählen Sie eine beliebige aus). Wählen Sie außerdem, falls Sie zur Auswahl des Formats des herunterzuladenden Zertifikats aufgefordert werden, das Standardformat aus.

---



Secure meetings

Authentication & Authorization

Administrators

Authentication Servers

Authorization Groups

Import Users

Active Users

Network

Network Settings

Clustering

Web Proxy

Email Settings

SNMP

### New Certificate Signing Request

Use this page to create a new Certificate Signing Request (CSR) to send to your Certificate Authority of choice.

Common Name:  
(e.g., secure.company.com)

iveserver.yourcompany.co

Organization Name:  
(e.g., Company Inc.)

YourCompany, Inc.

Org. Unit Name:  
(e.g., IT Group)

IT

Locality:  
(e.g., SomeCity)

Sunnyvale

State (fully spelled out):  
(e.g., California)

California

Country (2 letter code):  
(i.e., US)

US

Email Address:

it@yourcompany.com

Please enter some random characters to augment the system's random key generator. We recommend that you enter approximately twenty characters.

Random Data:  
(used for key generation)

\*\*\*\*\*

Create CSR

Abbildung 26: System > Certificates > Server Certificate > New CSR...

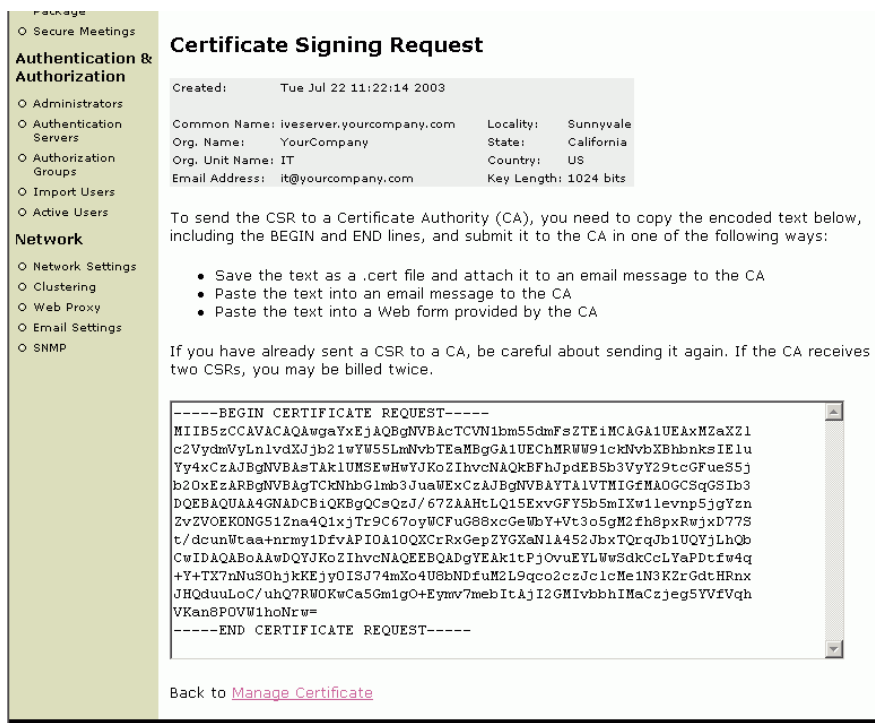


Abbildung 27: System > Certificates > Server Certificate > New Certificate Signing Request > Create CSR ...

## ☒ Importieren eines signierten Serverzertifikats, das anhand einer Zertifikatssignaturanforderung erstellt wurde

Falls Sie eine Zertifikatssignaturanforderung über die Administratorkonsole erstellen, wird auf der Registerkarte **Server Certificate** das Formular **Import the Certificate for a pending CSR** angezeigt.

### So importieren Sie ein signiertes Serverzertifikat, das anhand einer Zertifikatssignaturanforderung erstellt wurde

1. Klicken Sie in der Administratorkonsole auf die Registerkarte **System > Certificates > Server Certificate**.
2. Wechseln Sie unter **Import the Certificate for a pending CSR** zu der Zertifikatsdatei, die Sie von der Zertifizierungsstelle erhalten haben, und klicken Sie dann auf **Import**.

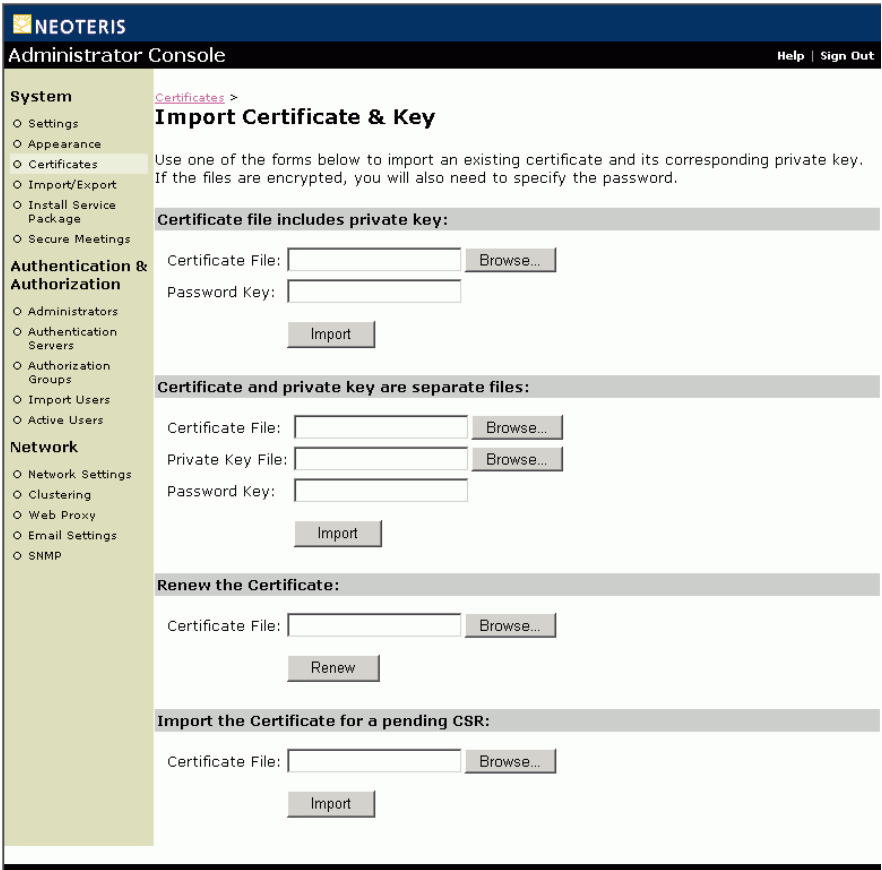


Abbildung 28: System > Certificates > Server Certificate > Import / Renew ...  
(nach dem Erstellen einer Zertifikatssignaturanforderung)

## Registerkarte „CA Certificate“

### ☒ Importieren eines Stammzertifikats zur Überprüfung eines clientseitigen Zertifikats

Falls Sie festlegen, dass die Benutzer zur Anmeldung am IVE ein clientseitiges Zertifikat angeben müssen, müssen Sie ein Stammzertifikat angeben. Anhand des Stammzertifikats wird überprüft, ob das vom Browser bereitgestellte Zertifikat gültig ist. In diesem Abschnitt wird erläutert, wie Sie das Stammzertifikat importieren.

---

**Hinweis:** Falls das Zertifikat verkettet ist, importiert das IVE nur das Stammzertifikat. Zur Überprüfung des importierten Zertifikats klicken Sie auf der Seite **Certificates > CA Certificate** auf die Verknüpfung **Certificate Details**. Obwohl das IVE nur das Stammzertifikat importiert, können Sie weiterhin eine Authentifizierung anhand eines verketteten Zertifikats durchführen, indem Sie dieses im Browser eines Benutzers installieren. Falls der Browser eines Benutzers über ein verkettetes Zertifikat verfügt, führt das IVE die Authentifizierung anhand des Stammzertifikats durch. Danach werden die Zwischenzertifikate aus dem Browser zwischengespeichert, die während der Sitzung verwendet werden sollen.

---

Um den Zugriff für eine Autorisierungsgruppe weiter zu beschränken, geben Sie wie in „Überprüfen der Zuordnungen von Servern zu Gruppen“ auf Seite 137 beschrieben die zur Authentifizierung erforderlichen X.509-DN-Attribute (Distinguished Name) ein. Beispielsweise möchten Sie dasselbe Zertifikat zwar für mehrere Arbeitsgruppen verwenden, den Zugriff auf eine bestimmte Ressource jedoch durch die Anforderung beschränken, dass das Zertifikat eines Benutzer bestimmte DN-Attribute besitzen muss.

### So geben Sie ein Stammzertifikat an

1. Klicken Sie in der Administratorkonsole auf die Registerkarte **System > Certificates > CA Certificate**.
2. Klicken Sie auf **Import Certificate**.
3. Wechseln Sie zu der Datei mit dem signierten Zertifikat für das Stammzertifikat, und klicken Sie auf **Import**.

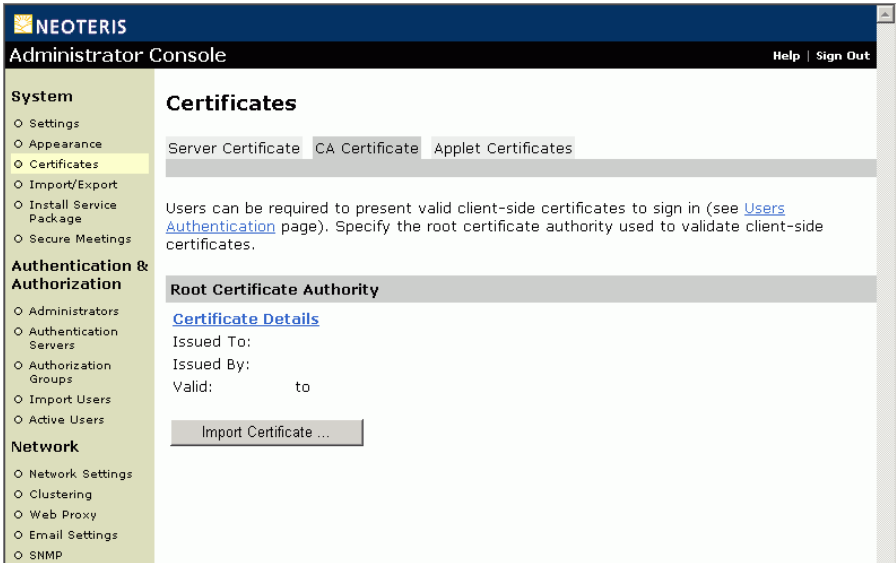


Abbildung 29: System > Certificates > CA Certificate

## Registerkarte „Applet Certificates“

Wenn das IVE ein signiertes Java-Applet vermittelt, signiert es das Applet mit einem eigenen Zertifikat neu, das nicht an ein Standardstammzertifikat gebunden ist. Wenn ein Benutzer ein Applet anfordert, das Aufgaben mit einem hohen Risikopotential durchführt, z. B. Zugreifen auf Netzwerkserver, wird im Browser des Benutzers in einer Sicherheitswarnung angezeigt, dass der Stamm nicht vertrauenswürdig ist. Um die Anzeige dieser Warnung zu vermeiden, können Sie ein Codesignaturzertifikat anfordern, mit dem das IVE zu vermittelnde Applets neu signiert.

Folgende Codesignaturzertifikate werden unterstützt:

- **Microsoft Authenticode-Zertifikat**

Mit diesem Zertifikat signiert das IVE Applets, die über MS JVM ausgeführt werden.

- **Microsoft Authenticode-Zertifikat (Mehrzweck)**

Mit diesem Zertifikat signiert das IVE Applets, die über MS JVM oder SUN JVM ausgeführt werden.

- **JavaSoft-Zertifikat**

Mit diesem Zertifikat signiert das IVE Applets, die über SUN JVM ausgeführt werden.

Beachten Sie bei der Auswahl des zu importierenden Codesignaturzertifikats folgende Browserabhängigkeiten:

- **Internet Explorer**

Auf neuen Computern, auf denen bei der Lieferung Windows XP vorinstalliert ist, wird in Internet Explorer normalerweise die SUN JVM ausgeführt. Dies bedeutet, dass Applets vom IVE mit dem Microsoft Authenticode-Zertifikat (Mehrzweck) oder dem JavaSoft-Zertifikat neu signiert werden müssen.

Auf PCs unter Windows 98 oder 2000 oder auf PCs, die auf Windows XP aktualisiert wurden, wird in Internet Explorer normalerweise die MS JVM ausgeführt. Dies bedeutet, dass Applets vom IVE mit einem der Authenticode-Zertifikate neu signiert werden müssen.

- **Netscape**

Netscape-Browser unterstützen nur die SUN JVM. Dies bedeutet, dass Applets vom IVE mit dem JavaSoft-Zertifikat neu signiert werden müssen.

## ☑ Importieren eines Codesignaturzertifikats

Mit Hilfe der Registerkarte **Applet Certificate** können Sie die geeigneten Zertifikate für die Benutzer importieren. Achten Sie darauf, dass Sie außerdem für die entsprechenden Autorisierungsgruppen die Unterstützung von Java-Applets aktiviert haben. Weitere Informationen finden Sie unter „Enable Java Applet Support“ auf Seite 149.

### Weitere Hinweise für Benutzer der SUN JVM:

- Standardmäßig werden Applets vom Java-Plug-In zusammen mit dem Codesignaturzertifikat zwischengespeichert, das beim Benutzerzugriff auf das Applet bereitgestellt wird. Dieses Verhalten bedeutet, dass der Browser Applets auch nach dem Importieren eines Codesignaturzertifikats in das IVE weiterhin mit dem ursprünglichen Zertifikat bereitstellt. Um sicherzustellen, dass Benutzer der SUN JVM keine Aufforderungen für nicht vertrauenswürdige Zertifikate für Applets erhalten, auf die sie vor dem Import eines Codesignaturzertifikats zugegriffen haben, muss der Cache des Java-Plug-Ins geleert werden. Alternativ können Benutzer den Cache deaktivieren. Durch diese Option kann jedoch die Leistung beeinträchtigt werden, da das Applet bei jedem Benutzerzugriff abgerufen werden muss.
- Das Java-Plug-In verwaltet eine eigene Liste vertrauenswürdiger Webserverzertifikate, die sich von der entsprechenden Liste des Browsers unterscheidet. Wenn ein Benutzer auf ein Applet zugreift, stellt die SUN JVM (zusätzlich zum Browser) eine eigene Verbindung mit dem Webserver her, auf dem sich das Applet befindet. Dem Benutzer wird daraufhin die Option zur Verfügung gestellt, zusätzlich zum Codesignaturzertifikat das Webserverzertifikat anzunehmen. In solchen Fällen muss der Benutzer die Schaltfläche **Always Trust** für das Webserverzertifikat auswählen. Aufgrund einer integrierten Zeitüberschreitung im Java-Plug-In wird das Applet nicht geladen, wenn der Benutzer bei der Auswahl dieser Schaltfläche für das Webserverzertifikat zu lange wartet.

### So importieren Sie ein Codesignaturzertifikat

1. Klicken Sie in der Administratorkonsole auf die Registerkarte **System > Certificates > Applet Certificates**.
2. Klicken Sie unter **Applet Signing Certificates** auf **Import Certificates**.
3. Wechseln Sie auf der Seite **Import Certificates** zu den entsprechenden Dateien mit dem Codesignaturzertifikat, geben Sie die Informationen für den Kennwortschlüssel ein, und klicken Sie dann auf **Import**.

4. Geben Sie auf der Registerkarte **Applet Certificates** die Server ein, deren Applets Sie als vertrauenswürdig einstufen möchten. Sie können die IP-Adresse oder den Domännennamen eines Servers eingeben.

Das IVE signiert nur Applets neu, die von vertrauenswürdigen Servern stammen. Wenn ein Benutzer ein Applet anfordert, das von einem nicht in der Liste aufgeführten Server stammt, verwendet das IVE nicht die importierten Produktionszertifikate zum Signieren des Applets. Dies bedeutet, dass dem Benutzer im Browser eine Sicherheitswarnung angezeigt wird.

---

**Hinweis:** Für Benutzer der Sun JVM überprüft das IVE außerdem, ob die Stammzertifizierungsstelle des ursprünglichen Appletzertifikats in der Liste vertrauenswürdiger Stammzertifizierungsstellen aufgeführt ist.

---





Abbildung 30: System > Certificates > Applet Certificates

## System > Menü „Import/Export“

Auf den Registerkarten **Import/Export** können Sie folgende Einstellungen speichern:

- **Systemkonfigurationseinstellungen (58) und Datensätze für lokale Benutzerkonten (60)**

Diese Informationen werden in einer verschlüsselten Datei unter dem angegebenen Pfad gespeichert. Informationen zum Festlegen eines Archivierungsplans für die Systemkonfiguration und Benutzerkonten finden Sie unter „Planen der Archivierung von Systeminformationen“ auf Seite 24.

- **Zugriffssteuerungslisten (ACLs) für Autorisierungsgruppen und Lesezeichen (62)**

Diese Informationen werden in einer XML-Datei unter dem angegebenen Pfad gespeichert. Sie können die XML-Datei bearbeiten, um ACLs und Lesezeichen für eine Autorisierungsgruppe hinzuzufügen, zu ändern oder zu löschen, und dann die überarbeiteten ACLs und Lesezeichen in die Gruppe importieren. Diese Informationen bilden einen Teil der Systemkonfigurationseinstellungen.

## Registerkarte „Configuration“

Mit Hilfe dieser Registerkarte können Sie eine Systemkonfigurationsdatei importieren oder exportieren. Die Systemkonfigurationsdatei enthält alle systemweiten Einstellungen für Authentifizierungsserver, Autorisierungsgruppe und Netzwerk.

### ☒ Exportieren einer Systemkonfigurationsdatei

#### So exportieren Sie eine Systemkonfigurationsdatei

1. Wählen Sie in der Administratorkonsole **System > Import/Export > Configuration** aus.
2. Geben Sie unter **Export** ein Kennwort ein, wenn die Konfigurationsdatei durch ein Kennwort geschützt werden soll.
3. Klicken Sie zum Speichern der Datei auf **Save Config As**.

## ☑ Importieren einer Systemkonfigurationsdatei

Beim Importieren einer Systemkonfigurationsdatei können Sie das Serverzertifikat und die IP-Adresse oder die Netzwerkeinstellungen des IVE-Servers aus den importierten Informationen ausschließen. Um beispielsweise mehrere IVEs hinter einem Load-Balancer einzurichten, importieren Sie alle Daten außer der IP-Adresse. Um ein IVE als Sicherungsserver einzurichten, importieren Sie alle Daten außer dem digitalen Zertifikat und den Netzwerkeinstellungen.

### So importieren Sie eine Konfigurationsdatei

1. Wählen Sie in der Administratorkonsole **System > Import/Export > Configuration** aus.
2. Geben Sie an, ob Sie das Serverzertifikat importieren möchten. Das Zertifikat wird nur importiert, wenn Sie das Kontrollkästchen **Import Server Certificate?** aktivieren.
3. Wählen Sie eine Importoption aus. Beachten Sie folgende Punkte:
  - Wenn Sie die IP-Adresse ausschließen, wird die IP-Adresse des Servers beim Importieren der Datei nicht geändert.
  - Wenn Sie die Netzwerkeinstellungen ausschließen, werden die Informationen auf der Seite **Network Settings** (interner Port, externer Port und statische Routeneinstellungen) nicht geändert.
4. Wechseln Sie zu der Konfigurationsdatei, die in der Standardeinstellung `system.cfg` heißt.
5. Geben Sie das für die Datei festgelegte Kennwort ein. Wenn Sie vor dem Export der Datei kein Kennwort festgelegt haben, lassen Sie dieses Feld leer.
6. Klicken Sie auf **Import Config**.

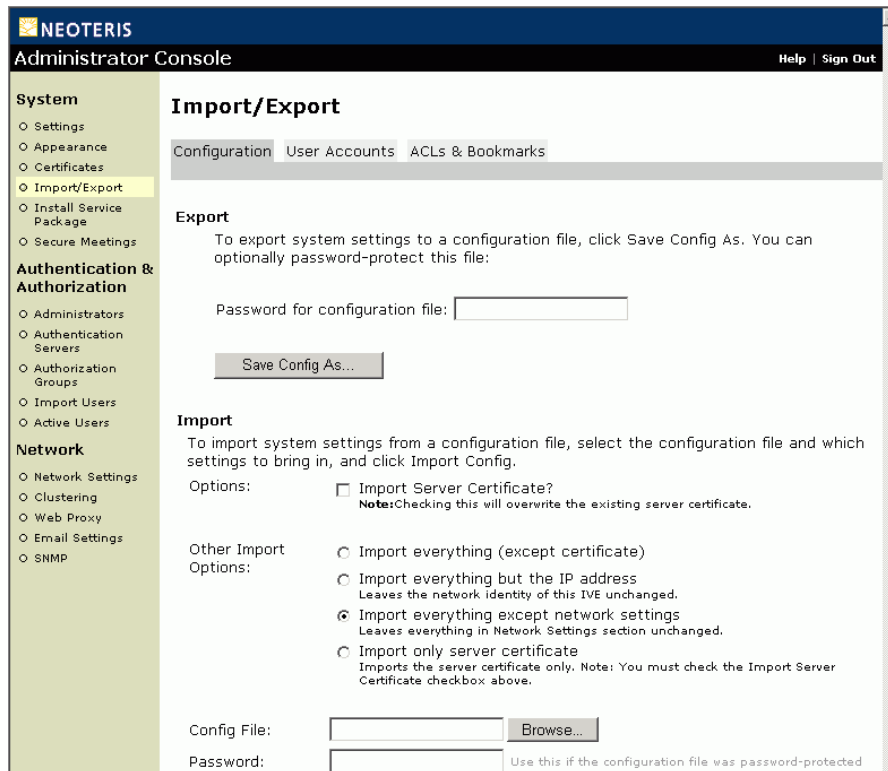


Abbildung 31: System > Import/Export > Registerkarte „Configuration“

## Registerkarten „User Accounts“

Mit Hilfe dieser Registerkarte können Sie lokale Benutzerkonten importieren oder exportieren. In der Benutzerkontendatei sind sämtliche lokalen Benutzer enthalten, die Sie für alle lokalen Authentifizierungsserver definiert haben.

### ☒ Exportieren lokaler Benutzerkonten

#### So exportieren Sie eine Systemkonfigurationsdatei

1. Wählen Sie in der Administratorkonsole **System > Import/Export > Configuration** aus.

2. Geben Sie unter **Export** ein Kennwort ein, wenn die Konfigurationsdatei durch ein Kennwort geschützt werden soll.
3. Klicken Sie zum Speichern der Datei auf **Save Config As**.

## ☑ Importieren lokaler Benutzerkonten

### So importieren Sie lokale Benutzerkonten

1. Wählen Sie in der Administratorkonsole **System > Import/Export > User Accounts** aus.
2. Wechseln Sie zu der Konfigurationsdatei, die in der Standardeinstellung `user.cfg` heißt.
3. Geben Sie das für die Datei festgelegte Kennwort ein. Wenn Sie vor dem Export der Datei kein Kennwort festgelegt haben, lassen Sie dieses Feld leer.
4. Klicken Sie auf **Import Config**.

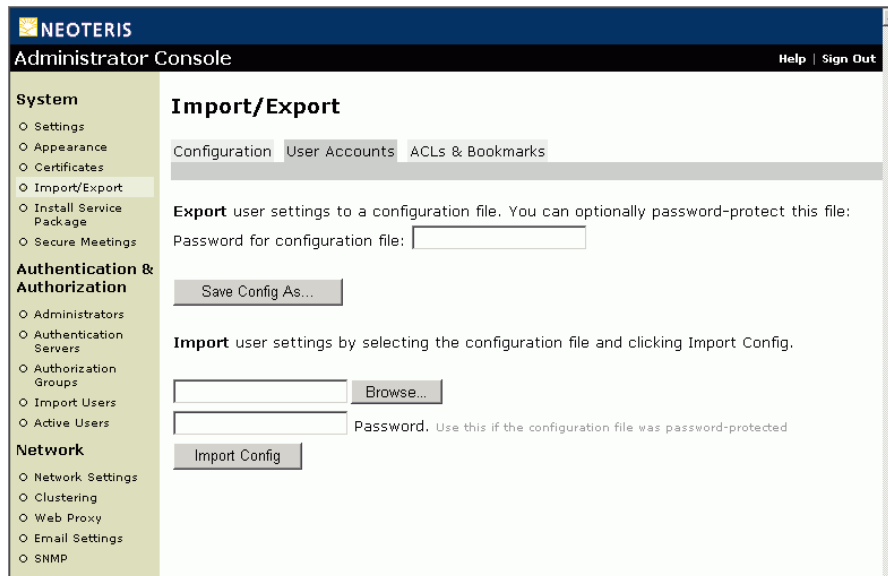


Abbildung 32: System > Import/Export > Registerkarte „User Accounts“

## Registerkarte „ACLs & Bookmarks“

Mit Hilfe dieser Registerkarte können Sie Zugriffssteuerungslisten (ACLs) und Lesezeichen für Autorisierungsgruppen importieren oder exportieren. Die Daten werden als XML-Datei exportiert, die für jede exportierte Gruppe ein `<group>`-Element in folgendem Format enthält:

```
<?xml version="1.0"?>
<Config>
  <Groups>
    <Group Name="Users">
      ...
    </Group>
    <Group Name="custom_group">
      ...
    </Group>
  </Groups>
</Config>
```

Jedes `<group>`-Element enthält Elemente für jeden Typ von ACL und Lesezeichen, der für die Gruppe konfiguriert ist. Die Details für ACLs und Lesezeichen werden durch geschachtelte Elemente dargestellt. Zu diesen zählen:

```
<webBookmark>
  <Url>http://www.ihrefirma.com</Url>
  <Name>http://www.ihrefirma.com</Name>
  <Description>Dies ist Ihre Startseite.</Description>
  <StartPage>Nr</StartPage>
</webBookmark>
```

Sie können die ACLs und Lesezeichen einer Gruppe problemlos bearbeiten, indem Sie die entsprechenden Elemente ändern, hinzufügen oder löschen. Wenn Sie die überarbeitete XML-Datei importieren, werden die vorhandenen ACLs und Lesezeichen durch die Elemente in der Datei **überschrieben**. Folgende Gruppeneinstellungen sollten Sie ebenfalls beachten:

- **Vererbung**

Wenn eine benutzerdefinierte Autorisierungsgruppe für die Verwendung der Gruppeneinstellungen für Benutzer konfiguriert ist, bleiben die vererbten ACLs und Lesezeichen weiterhin gültig. Wenn Sie die Gruppe für die Verwendung benutzerdefinierter Einstellungen konfigurieren, werden die zuletzt importierten ACLs und Lesezeichen verwendet.

- **Offene oder geschlossene Richtlinie**

Das IVE importiert und exportiert alle angegebenen ACLs und Lesezeichen für eine Gruppe unabhängig von den zugeordneten Richtlinien. Wenn die Gruppe mit einer offenen Richtlinie konfiguriert wurde, gelten die zugeordneten ACLs und Lesezeichen. Wenn die Gruppe mit einer geschlossenen Richtlinie konfiguriert wurde, gelten die ACLs und Lesezeichen, die für die geschlossene Richtlinie konfiguriert wurden.

## Primäre ACL- und Lesezeichenelemente

Die folgenden Elemente werden für Autorisierungsgruppen unterstützt:

- **<webAcls>**: Enthält die Details der Web-ACL für eine Gruppe
  - **<Type>**: Die offene oder geschlossene Zugriffsrichtlinie, die die Ressourcen steuert, auf die Benutzer zugreifen können
  - **<RawIP>**: Die allgemeine IP-Richtlinie (Gewähren oder Verweigern), die steuert, ob Benutzer über die IP-Adresse des Servers auf eine Ressource zugreifen können
  - **<Open>**: Die Ausnahmeliste für eine offene Richtlinie, die aus **<webAcl>**-Elementen besteht
  - **<Closed>**: Die Ausnahmeliste für eine geschlossene Richtlinie, die aus **<webAcl>**-Elementen besteht
- **<windowsAcls>**: Enthält die Details der Windows-ACL für eine Gruppe
  - **<Type>**: Die offene oder geschlossene Zugriffsrichtlinie, die die Ressourcen steuert, auf die Benutzer zugreifen können
  - **<RawIP>**: Die allgemeine IP-Richtlinie (Gewähren oder Verweigern), die steuert, ob Benutzer über die IP-Adresse des Servers auf eine Ressource zugreifen können
  - **<Grant>**: Die Ausnahmeliste für eine geschlossene Richtlinie, die aus **<windowsAcl>**-Elementen besteht
  - **<Deny>**: Die Ausnahmeliste für eine offene Richtlinie, die aus **<windowsAcl>**-Elementen besteht
- **<nfsAcls>**: Enthält die Details der NFS-ACL für eine Gruppe
  - **<Grant>**: Die aus **<nfsAcl>**-Elementen bestehenden UNIX-Hosts, auf die Benutzer zugreifen können
- **<SAMapps>**: Enthält eine Liste der **<SAMApp>**-Elemente (d. h. Anwendungen, auf die die Gruppe über Secure Application Manager zugreifen kann)
- **<webBookmarks>**: Enthält eine Liste von **<webBookmark>**-Elementen
- **<windowsBookmarks>**: Enthält eine Liste von **<windowsBookmark>**-Elementen
- **<nfsBookmarks>**: Enthält eine Liste von **<nfsBookmark>**-Elementen

## ☑ Exportieren von ACLs und Lesezeichen

Sie können den Datentyp festlegen, der für alle Gruppen oder für eine bestimmte Gruppe exportiert werden soll. Wenn Sie alle ACLs und Lesezeichen für alle Gruppen exportieren, können Sie die Daten einzeln festlegen, die für eine ausgewählte Gruppe importiert werden sollen.

### So exportieren Sie ACLs und Lesezeichen

1. Wählen Sie in der Administratorkonsole **System > Import/Export > ACLs & Bookmarks** aus.
2. Wählen Sie im Dropdownmenü **Groups** den Eintrag **All Groups** oder eine einzelne Gruppe aus.
3. Wählen Sie im Dropdownmenü **Data** den Typ der zu exportierenden Daten aus. Sie können mehrere Optionen auswählen, indem Sie die STRG-TASTE verwenden.
4. Klicken Sie zum Speichern der Datei auf **Save Config As**.

## ☑ Importieren von ACLs und Lesezeichen

Sie können den Typ von ACL-Daten und Lesezeichendaten angeben, der für eine Gruppe aus einer XML-Datei importiert werden soll, die das <group>-Element der Gruppe enthält. Wenn die XML-Datei kein <group>-Element für eine vorhandene Gruppe enthält, können Sie der Datei dieses Element sowie die gewünschten ACL-Daten und Lesezeichendaten hinzufügen. Sie können jedoch keine neue Autorisierungsgruppe für das IVE erstellen, indem Sie der XML-Datei ein <group>-Element für die neue Gruppe hinzufügen und diese anschließend importieren.

---

**Wichtig:** Wenn Sie ACL-Daten und Lesezeichendaten in eine Gruppe importieren, werden die vorhandenen Konfigurationsinformationen durch die importierten Informationen **überschrieben** (sie werden nicht angehängt).

---



## So importieren Sie ACLs und Lesezeichen

1. Wählen Sie in der Administratorkonsole **System > Import/Export > ACLs & Bookmarks** aus.
2. Wählen Sie im Dropdownmenü **Groups** die Gruppe aus, in die Sie die ACLs und Lesezeichen importieren möchten.
3. Wählen Sie im Dropdownmenü **Data** die Konfigurationsdaten für ACLs und Lesezeichen aus, die Sie in die angegebene Gruppe importieren möchten.
4. Wechseln Sie zu der zuvor gespeicherten Konfigurationsdatei, und klicken Sie dann auf **Import Config**.

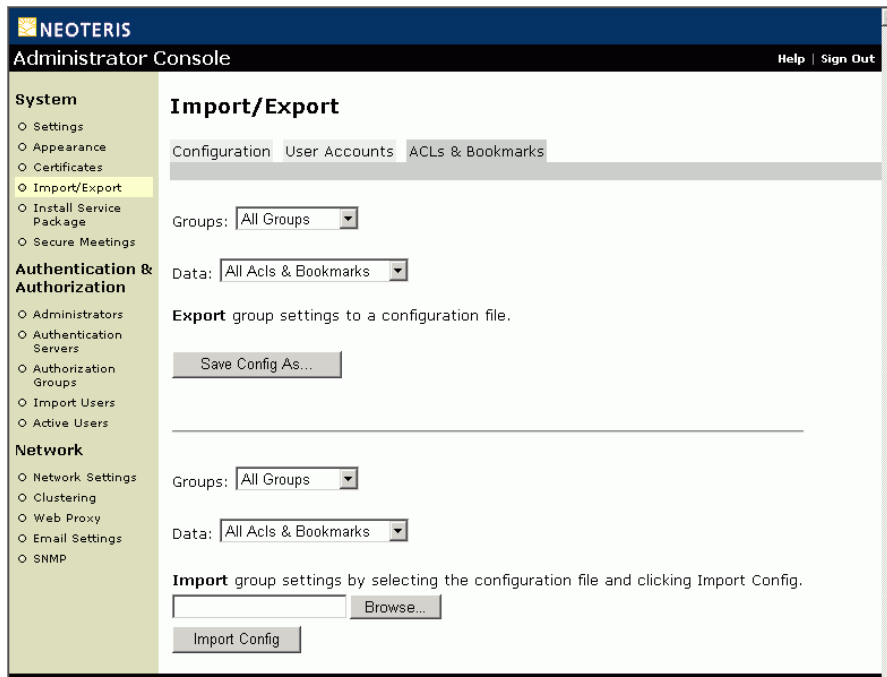


Abbildung 33: System > Import/Export > ACLs & Bookmarks

## System > Menü „Install Service Package“

Sie können ein anderes Dienstpaket installieren, indem Sie zuerst von der Neoteris-Support-Website die Software herunterladen und diese dann über die Administratorkonsole hochladen. Dieses Feature wird meist dazu verwendet, Aktualisierungen auf neuere Versionen der Systemsoftware durchzuführen. Sie können jedoch mit diesem Verfahren die Systemsoftware auch auf eine ältere Version herunterstufen oder alle aktuellen Konfigurationseinstellungen löschen und eine neue Ausgangsbasis schaffen. Paketdateien werden verschlüsselt und signiert, so dass der IVE-Server nur gültige, von Neoteris ausgegebene Pakete akzeptiert. Mit dieser Maßnahme wird verhindert, dass der IVE-Server als „Trojanische Pferde“ bezeichnete Programme akzeptiert.

### ☒ Installieren eines Neoteris-Softwaredienstpakets

#### So installieren Sie ein Dienstpaket

1. Wechseln Sie zur Neoteris-Support-Website <http://support.neoteris.com>, und rufen Sie das gewünschte Dienstpaket ab.
2. Wählen Sie in der Administratorkonsole das Menü **System > Install Service Package** aus.
3. Klicken Sie auf **Browse**, um das von der Supportsite heruntergeladene Dienstpaket auf der Festplatte zu suchen. Wenn Sie die aktuellen Konfigurationseinstellungen löschen, aber weiterhin dieselbe IVE-Version verwenden möchten, wählen Sie das derzeit in Ihrem IVE installierte Dienstpaket aus.
4. Wenn Sie die Software auf ein älteres Dienstpaket herunterstufen oder die Konfigurationseinstellungen löschen, wählen Sie **Delete all system and user data**.

---

**Wichtig:** Wenn Sie das IVE zurücksetzen und mit dieser Option alle System- und Benutzerdaten aus dem IVE löschen möchten, müssen Sie vor der erneuten Systemkonfiguration die Netzwerkverbindungen wiederherstellen. Beachten Sie außerdem, dass das IVE nicht auf eine ältere Version als 3.1 zurückgestuft werden kann.

---

5. Wählen Sie die Dienstpaketdatei aus, und klicken Sie auf **Install**.

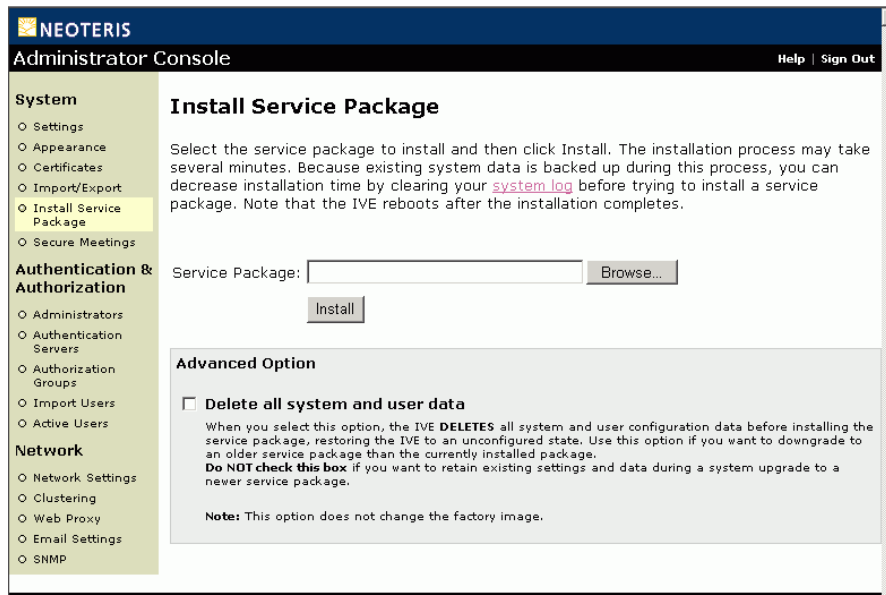


Abbildung 34: System &gt; Install Service Package

## System > Menü „Secure Meetings“

Secure Meeting ermöglicht es, eine Auswahl von Benutzern im Internet einzuladen, mit diesen Konferenzen durchzuführen und Ihren Desktop oder Ihre Desktopanwendungen für diese Benutzer freizugeben. Bei Verwendung von Secure Meeting gilt Folgendes:

- IVE-Benutzer können sowohl IVE-Benutzer als auch andere Personen zur Teilnahme an sicheren Online-Konferenzen einladen.
- Während der Konferenzen können die Vorführenden ihre Desktops und Anwendungen für andere Teilnehmer freigeben.
- Konferenzteilnehmer können mit Hilfe von Tools für Textnachrichten problemlos mit der Gruppe chatten.

Zusätzlich zu verschiedenen E-Mail- und Kalendertools sowie weiteren Tools und Features enthält Secure Meeting folgende wichtigen Sicherheitsfeatures:

- Administratoren können Konferenzen auf registrierte IVE-Benutzer beschränken.
- Administratoren können die Funktion für externe Benutzer deaktivieren, den Desktop des Vorführenden remote zu steuern.

Mit den Einstellungen im Menü **Secure Meetings** können Sie Secure Meeting so konfigurieren, dass Gäste automatisch E-Mail-Nachrichten mit Konferenzdetails erhalten und dass alle derzeit auf dem IVE-Server geplanten Konferenzen angezeigt werden.

---

**Wichtig:** Bei Verwendung von Secure Meeting in Verbindung mit einem SSL-Zertifikat im IVE wird die Installation eines Zertifikats auf Produktionsebene empfohlen. Wenn Sie ein selbst signiertes SSL-Zertifikat installieren, können für Secure Meeting-Benutzer möglicherweise Schwierigkeiten bei der Konferenzanmeldung auftreten. Insbesondere kann den Konferenzteilnehmern eine Fehlermeldung „Cannot Connect to the Secure Meeting server...“ angezeigt werden. Wenn Sie ein selbst signiertes Zertifikat verwenden möchten, weisen Sie die Konferenzteilnehmer an, bei Anzeige der Fehlermeldung auf **View Certificate** und dann auf **Install Certificate** zu klicken, um das Zertifikat vor dem Beitreten der Konferenz zu installieren. Weitere Informationen finden Sie in der Übersicht über Zertifikate in „System > Menü „Certificates““ auf Seite 41.

---

## Registerkarte „General“

### ☒ Aktivieren von E-Mail-Benachrichtigungen für Konferenzen

Auf der Registerkarte **General** können Sie automatische E-Mail-Benachrichtigungen an Gäste von Secure Meeting aktivieren bzw. deaktivieren. Beachten Sie, dass für Secure Meeting zum Weiterleiten von E-Mail-Nachrichten ein SMTP-Server verwendet werden muss, auf den vom IVE aus zugegriffen werden kann.

#### So aktivieren Sie automatische E-Mail-Benachrichtigungen für Konferenzgäste

1. Klicken Sie in der Administratorkonsole auf die Registerkarte **System > Secure Meetings > General**.
2. Wählen Sie **Enabled** aus.
3. Geben Sie im Feld **SMTP Server** die IP-Adresse oder den Hostnamen eines SMTP-Servers ein, der E-Mail-Nachrichten vom IVE an die Konferenzgäste weiterleiten kann.
4. Geben Sie bei entsprechender Anforderung vom SMTP-Server in den Feldern **SMTP Login** und **SMTP Password** einen gültigen Anmeldenamen und ein Kennwort für den angegebenen E-Mail-SMTP-Server ein.

5. Geben Sie im Feld **SMTP Email** Ihre E-Mail-Adresse oder die Adresse eines anderen Administrators ein. Secure Meeting verwendet die angegebene Adresse als E-Mail-Adresse des Absenders, wenn der Ersteller der E-Mail-Nachricht keine eigene E-Mail-Adresse im IVE festlegt.
6. Klicken Sie auf **Save Changes**.
7. Konfigurieren Sie Secure Meeting-Einstellungen für einzelne Autorisierungsgruppen anhand der Anweisungen in „Ermöglichen und Konfigurieren von Konferenzen für Autorisierungsgruppen“ auf Seite 216.

### So deaktivieren Sie automatische E-Mail-Benachrichtigungen für Konferenzgäste

1. Klicken Sie in der Administratorkonsole auf die Registerkarte **System > Secure Meetings > General**.
2. Wählen Sie **Disabled** aus.
3. Klicken Sie auf **Save Changes**.

**NEOTERIS**  
Administrator Console Help | Sign Out

**System**

- Settings
- Appearance
- Certificates
- Import/Export
- Install Service Package
- Secure Meetings

**Authentication & Authorization**

- Administrators
- Authentication Servers
- Authorization Groups
- Import Users
- Active Users

**Network**

- Network Settings
- Clustering
- Web Proxy
- Email Settings
- SNMP

General Schedule

Save Changes

**Email meeting notifications**

Email notifications allow meeting creators to easily notify invitees with known email addresses of new or modified meetings. If you enable email notifications, you must specify an SMTP server that is accessible by the IVE.

\* indicates required field

☒ Enabled

SMTP Server: \*  Name or IP address

SMTP Login:  Username used to access the server

SMTP Password:  Password used to access the server

SMTP Email: \*  Email address for bounced mail

☐ Disabled

Save Changes

Abbildung 35: System > Secure Meetings > General


## Registerkarte „Schedule“

### ☒ Anzeigen und Absagen geplanter Konferenzen

Auf dieser Registerkarte können Sie alle derzeit auf dem IVE-Server geplanten Konferenzen anzeigen und ggf. Konferenzen absagen.

#### So zeigen Sie Konferenzen an

1. Klicken Sie in der Administratorkonsole auf die Registerkarte **System > Secure Meetings > General**. Im IVE werden Echtzeitinformationen zu allen derzeit ausgeführten oder geplanten Konferenzen angezeigt.
2. Gehen Sie zum Ändern der Konferenzansicht wie folgt vor:
  - Wählen Sie in der Liste **View** einen Zeitraum aus, und klicken Sie auf **Update**, um zu steuern, welche Konferenzen angezeigt werden.
  - Klicken Sie auf eine beliebige unterstrichene Spaltenüberschrift, um die Sortierreihenfolge der derzeit angezeigten Konferenzen zu steuern.

Wenn Sie eine Konferenz absagen möchten, klicken Sie rechts neben dem Konferenzstatus auf das  Symbol zum Löschen.

## Kapitel3

# Verwalten der Authentifizierung und Autorisierung für IVE

Die Verwaltung des IVE umfasst die Konfiguration und Verwaltung von systemweiten Einstellungen, Authentifizierungsservern, Autorisierungsgruppen und Netzwerkeinstellungen. In diesem Kapitel werden Authentifizierung und Autorisierung für Benutzer und die Features beschrieben, die auf Gruppenebene aktiviert werden können. Außerdem werden Vorgehensweisen zum Konfigurieren von Authentifizierungsservern und von Einstellungen für Autorisierungsgruppen bereitgestellt.

---

**Wichtig:** Wenn Sie derzeit IVE der Version 2.x ausführen, wenden Sie sich an den Neoteris-Support, um wichtige Informationen zu den Auswirkungen einer Aktualisierung auf Version 3.0 für das System und die Benutzerdaten zu erhalten.

---

### Übersichtsinformationen finden Sie unter:

Übersicht über Authentifizierung und Autorisierung .....	72
Unterstützte Authentifizierungsserver .....	75

### Informationen zur Vorgehensweise finden Sie unter:

Authentication & Authorization > Menü „Administrators“ .....	82
Authentication & Authorization > Menü „Authentication Servers“ .....	92
Menü „Authentication & Authorization > Authorization Groups“ .....	126
Authentication & Authorization > Menü „Import Users“ .....	220
Authentication & Authorization > Menü „Active Users“ .....	223

## Übersicht über Authentifizierung und Autorisierung

IVE, Version 3.0, enthält im Vergleich zu früheren Versionen einen neuen AA-Vorgang (Authentifizierung und Autorisierung). Dieser AA-Vorgang wird einfach als **Standardmodus** für Systeme der Version 3.0+ behandelt. Wenn Sie eine Aktualisierung von einer vorhandenen 2.x-Konfiguration vornehmen, wenden Sie sich an den Neoteris-Support, bevor Sie vom Legacymodus in den Standardmodus wechseln.

---

**Hinweis:** Neuen Kunden des IVE wird dringend vom Aktivieren des Legacymodus abgeraten.

---

Wenn Sie den AA-Vorgang (Authentifizierung und Autorisierung) im IVE für Benutzer konfigurieren möchten, müssen Sie folgende Elemente festlegen:

- Authentifizierungsserver
- Autorisierungsgruppen

### Authentifizierungsserver

Bei einem **Authentifizierungsserver** handelt es sich um eine Datenbank, in der Anmeldeinformationen für Benutzer (Benutzername und Kennwort) und normalerweise Gruppeninformationen gespeichert werden. Wenn sich ein Benutzer im IVE anmeldet, muss er einen Authentifizierungsserver angeben, an den das IVE die Anmeldeinformationen senden soll. Der Authentifizierungsserver überprüft das Vorhandensein und die Identität des Benutzers. Nach der Überprüfung des Benutzers sendet der Authentifizierungsserver eine Genehmigung und bei entsprechender Konfiguration die Gruppeninformationen des Benutzers an das IVE. Das IVE weist den Benutzer dann einer Autorisierungsgruppe zu.

Das IVE unterstützt die folgenden Authentifizierungsserver:

- Lokaler IVE-Authentifizierungsserver ..... 75
- Active Directory oder Windows NT-Domäne ..... 75
- LDAP-Server ..... 76
- NIS-Server ..... 76
- RADIUS-Server ..... 77
- ACE/Server ..... 78

Um einen Authentifizierungsserver zu erstellen, müssen Sie den Server zunächst über die Optionen auf der Seite **Settings** einer Autorisierungsgruppe zuordnen. (Weitere Informationen finden Sie unter „Autorisierungsgruppen“ auf



Seite 73.) Wenn Sie anschließend die Servereinstellungen speichern, werden die folgenden Registerkarten angezeigt:

- **Group Mapping**

Auf der Registerkarte **Group Mapping** legen Sie Regeln fest, nach denen das IVE authentifizierte Benutzer einer IVE-Autorisierungsgruppe zuordnet.

- **Local Users**

Wenn Sie das lokale IVE als Authentifizierungsserver auswählen (anstelle eines externen Servers wie LDAP oder Radius), müssen Sie auf der Registerkarte **Local Users** eine lokale Datenbank für Benutzerdatensätze erstellen und dabei den Benutzernamen, den vollständigen Namen und das Kennwort jedes Benutzers festlegen. Auf der Seite **Local Users** werden folgende Elemente angezeigt:

- Lokale Benutzerkonten, wenn es sich bei dem Authentifizierungsserver um eine lokale (IVE-) Datenbank handelt. Auf dieser Seite können Sie lokale Benutzerkonten verwalten, also beispielsweise neue Konten erstellen, vorhandene Konten bearbeiten und lokale Benutzerkonten löschen.
- Benutzer, die sich im IVE angemeldet haben, wenn der Authentifizierungsserver ein externer Server ist. Um die Informationen zu Benutzerkonten im IVE auf dem aktuellen Stand zu halten, sollten Sie nach dem Entfernen eines Benutzers vom externen Authentifizierungsserver den entsprechenden Benutzernamen auf dieser Seite löschen.

- **User Admins**

Auf der Seite **User Admins** können Sie begrenzte Verwaltungsaufgaben an ausgewählte Endbenutzer delegieren. Insbesondere können Sie einzelnen Benutzern die Berechtigungen gewähren, auf der Startseite des sicheren Gateways über das Menü **User Admin** einem Authentifizierungsserver Benutzer hinzuzufügen sowie Benutzer zu löschen, die vollständigen Namen von Benutzern zu ändern und die Kennwörter von Benutzern zu ändern.

Informationen zum Konfigurieren eines Authentifizierungsservers finden Sie unter „Authentication & Authorization > Menü „Authentication Servers““ auf Seite 92.

## Autorisierungsgruppen

Eine **Autorisierungsgruppe** ist eine IVE-Benutzergruppe, der Sie authentifizierte Benutzer zuordnen können. Im IVE stehen drei Typen von Autorisierungsgruppen zur Verfügung:

- **Administratorengruppe**

Mitglieder der Administratorengruppe können sich an der Administratorkonsole anmelden und sämtliche System- und Benutzereinstellungen konfigurieren. Sie erstellen das erste Administratorengruppenkonto, wenn Sie über die serielle Konsole von Neoteris einen Benutzernamen und ein Kennwort angeben. Diese

Kontoinformationen werden auf dem lokalen IVE-Authentifizierungsserver gespeichert. Weitere Administratorkonten können Sie über die Administratorkonsole erstellen.

- **Benutzergruppe**  
Mitglieder der Benutzergruppe können sich bei der IVE-Startseite anmelden und die Features von Neoteris IVE verwenden, die Sie für die Benutzergruppe aktiviert haben.
- **Vom Administrator definierte Autorisierungsgruppe<sup>1</sup>**  
Bei einer vom Administrator definierten Autorisierungsgruppe handelt es sich lediglich um eine weitere Gruppe, für die bestimmte Zugriffssteuerungen verwendet werden. Benutzerdefinierte Autorisierungsgruppen erben in der Standardeinstellung die Einstellungen der Benutzergruppe.

Die Aufgabe einer Autorisierungsgruppe besteht im Festlegen der Ressourcen und Aufgaben, auf die Benutzer zugreifen und die sie durchführen können, z. B. Zugreifen auf bestimmte Webserver und Erstellen von Lesezeichen. Das IVE ordnet einen bestätigten Benutzer einer IVE-Autorisierungsgruppe basierend auf der Authentifizierungsserver**instanz** zu. Diese ist lediglich eine Konfiguration eines Servers, die die Serverinformationen und die Zuordnung von Benutzern zu Gruppen angibt. Die **Zuordnung von Benutzern zu Gruppen** ist die Methode, mit der das IVE authentifizierte Benutzer einer Autorisierungsgruppe zuordnet. Folgende Gruppenzuordnungsoptionen sind verfügbar:

- Das IVE erhält Gruppeninformationen aus der Authentifizierungstransaktion und ordnet den Benutzer basierend auf diesen Informationen einer Autorisierungsgruppe zu.

---

**Hinweis:** In Version 3.0 können Sie nur LDAP- und RADIUS-Server konfigurieren, um Gruppeninformationen als Teil des Transaktionsvorgangs zurückzugeben.

---

- Das IVE fragt einen weiteren externen Server nach den Gruppeninformationen des Benutzers ab.

---

**Hinweis:** In Version 3.0 wird nur ein LDAP-Verzeichnis für das externe Gruppenlookup unterstützt.

---

- Das IVE weist Benutzer Gruppen auf Grundlage des jeweiligen Benutzernamens zu.
- Das IVE weist alle Benutzer bestimmten Gruppen zu, die Sie jeweils als Teil dieser Option angeben.

Informationen zum Konfigurieren einer Autorisierungsgruppe finden Sie unter „Menü „Authentication & Authorization > Authorization Groups““ auf Seite 126.

---

1. Für Autorisierungsgruppen ist in einigen IVE-Produkten eine Lizenz erforderlich.

---

## Unterstützte Authentifizierungsserver

Das Neoteris IVE unterstützt die gängigsten Authentifizierungsserver, z. B. Windows NT-Domäne, Active Directory, RADIUS, LDAP, NIS und RSA ACE/Server. Sie können eine oder mehrere lokale Datenbanken für vom IVE authentifizierte Benutzer erstellen. Bei der Anmeldung im IVE müssen Benutzer die Authentifizierungsserverinstanz angeben, an die die Anmeldeinformationen gesendet werden sollen, indem sie die Instanz in einem Dropdownmenü auswählen (sofern Sie für das IVE-System mehrere Authentifizierungsserverinstanzen definiert haben). Anweisungen zum Erstellen einer Instanz finden Sie unter „Definieren einer Authentifizierungsserverinstanz“ auf Seite 92.

---

**Hinweis:** Ein Authentifizierungsserver muss eine Verbindung mit dem IVE-Server herstellen können. Wenn ein Authentifizierungsserver wie RSA ACE/Server keine IP-Adressen für die Agentenhosts verwendet, muss er den IVE-Hostnamen über einen DNS-Eintrag oder einen Eintrag in der eigenen Hostdatei auflösen können.

---

## Lokaler IVE-Authentifizierungsserver

Im IVE können Sie eine oder mehrere lokale Datenbanken für vom IVE authentifizierte Benutzer erstellen. Sie können lokale Benutzerdatensätze für Benutzer erstellen, die normalerweise von einem externen Authentifizierungsserver überprüft werden, den Sie deaktivieren möchten. Dies bietet sich auch an, wenn Sie eine Gruppe von temporären Benutzern erstellen möchten. Beachten Sie, dass alle Administratorenkonten als lokale Datensätze gespeichert werden, es jedoch möglich ist, dass Administratoren über einen externen Server authentifiziert werden. Weitere Informationen zur Administratorauthentifizierung finden Sie unter „Festlegen von IP-Adresseinschränkungen für die Administratorengruppe“ auf Seite 89. Konfigurationsinformationen finden Sie unter „Erstellen lokaler Benutzer (nur bei lokaler IVE-Authentifizierung)“ auf Seite 101.

## Active Directory oder Windows NT-Domäne

Beim Authentifizieren von Benutzern mit einem primären NT-Domänencontroller oder mit Active Directory melden sich Benutzer am Neoteris IVE-Server mit dem Benutzernamen und dem Kennwort an, mit denen sie auf den eigenen Windows-Desktop zugreifen. Konfigurationsinformationen finden Sie unter „Definieren einer Active Directory-Serverinstanz oder einer Windows NT-Domänenserverinstanz“ auf Seite 106.

## LDAP-Server

Beim Authentifizieren von Benutzern mit einem LDAP-Server überprüft der Neoteris IVE-Server vor dem Gewähren des Benutzerzugriffs, ob der auf der Anmeldeseite eingegebene Benutzername und das Kennwort im LDAP-Verzeichnis vorhanden sind. Beachten Sie, dass der an das IVE gesendete Benutzername kein Fragezeichen enthalten (?) darf.

Der Neoteris IVE-Server unterstützt drei LDAP-spezifische Authentifizierungsoptionen:

- **Unencrypted**—Benutzername und Kennwort werden an den LDAP-Verzeichnisdienst in einfachem Klartext gesendet.
- **LDAPS**—Die Daten in der LDAP-Authentifizierungssitzung werden mit dem SSL-Protokoll (Secure Socket Layer) verschlüsselt, bevor sie an den LDAP-Verzeichnisdienst gesendet werden.
- **LDAP over TLS**—Die Daten in der LDAP-Authentifizierungssitzung werden mit dem TLS-Protokoll (Transport Layer Security) verschlüsselt, bevor sie an den LDAP-Verzeichnisdienst gesendet werden.

Konfigurationsinformationen finden Sie unter „Festlegen einer LDAP-Serverinstanz“ auf Seite 108.

## NIS-Server

Beim Authentifizieren von Benutzern mit einem UNIX/NIS-Server überprüft der Neoteris IVE-Server, ob der auf der Anmeldeseite eingegebene Benutzername und das Kennwort einem gültigen Paar aus Benutzer-ID und Kennwort auf dem NIS-Server entsprechen. Beachten Sie, dass der an das IVE gesendete Benutzername keine zwei aufeinander folgenden Tilden (~~) enthalten darf.

---

**Hinweis:** Sie können nur eine NIS-Serverkonfiguration hinzufügen, mit der Sie jedoch eine beliebige Anzahl von Gruppen authentifizieren können.

---

Konfigurationsinformationen finden Sie unter „Festlegen einer NIS-Serverinstanz“ auf Seite 112.

## RADIUS-Server

Beim Authentifizieren von Benutzern mit einem RADIUS-Server müssen Sie den RADIUS-Server so konfigurieren, dass der Neoteris IVE-Server als Client erkannt wird. Außerdem müssen Sie für den RADIUS-Server einen gemeinsamen geheimen Schlüssel zur Verwendung bei der Authentifizierung der Clientanforderung angeben.

Der Neoteris IVE-Server unterstützt die RADIUS-Standardauthentifizierungsschemas. Zu diesen gehören folgende: Access-Request, Access-Accept und Access-Reject. Der Neoteris IVE-Server unterstützt nicht das erweiterte RADIUS-Authentifizierungsschema [Access-Challenge-Code], bei dem Benutzer zur Eingabe zusätzlicher Informationen aufgefordert werden. Wenden Sie sich an den Neoteris-Support, um weitere Informationen zu dieser Option zu erhalten.

Der Neoteris IVE-Server unterstützt auch RSA ACE/Server unter Verwendung des RADIUS-Protokolls und eines SecurID-Tokens (erhältlich von Security Dynamics). Wenn Sie für die Authentifizierung von Benutzern SecurID verwenden, müssen die Benutzer ihre Benutzer-ID und die Kombination aus PIN und dem Tokenwert angeben.

Wenn Sie einen PassGo Defender-RADIUS-Server verwenden, erfolgt die Benutzeranmeldung folgendermaßen:

1. Der Benutzer meldet sich beim IVE mit einem Benutzernamen und einem Kennwort an. Das IVE leitet diese Anmeldeinformationen an Defender weiter.
2. Defender sendet eine eindeutige Anfragezeichenfolge an das IVE, und im IVE wird diese Anfragezeichenfolge dem Benutzer angezeigt.
3. Der Benutzer gibt die Anfragezeichenfolge in einem Defender-Token ein, und das Token erzeugt eine Antwortzeichenfolge.
4. Der Benutzer gibt die Antwortzeichenfolge im IVE ein und klickt auf **Sign In**.

Konfigurationsinformationen finden Sie unter „Festlegen einer RADIUS-Serverinstanz“ auf Seite 113.

## ACE/Server

Beim Authentifizieren von Benutzern mit einem RSA ACE/Server können sich Benutzer mit zwei Methoden anmelden:

- **Unter Verwendung der IVE-Standardanmeldeseite:**  
Der Benutzer wechselt zur IVE-Standardanmeldeseite, gibt dann den Benutzernamen und das Kennwort ein (bestehend aus der Kombination von PIN und dem aktuellen Wert des RSA SecurID-Hardware- oder Softwaretokens). Das IVE leitet diese Anmeldeinformationen des Benutzers dann an ACE/Server weiter.
- **Unter Verwendung der RSA SecurID-Authentifizierungsseite:**  
Wenn der Benutzer RSA SecurID-Software im System installiert hat, kann er unter Verwendung des folgenden URL-Formats auf die Seite **RSA SecurID Authentication** wechseln: <https://IVE/login/ServerInstanz> und Eingabe der PIN. (In Abhängigkeit von der RSA-Konfiguration muss der Benutzer möglicherweise auch den Benutzernamen eingeben.) Wenn das IVE die Gültigkeit der Anmeldeanforderung bestätigt hat, kann die RSA SecurID-Software einen Tokenwert transparent über das IVE an ACE/Server weitergeben.

Wenn ACE/Server den Benutzer authentifiziert hat, wird der Zugriff auf das IVE gewährt. Andernfalls führt ACE/Server folgende Aktionen aus:

- **Verweigern des Benutzerzugriffs auf das System**  
wenn die Anmeldeinformationen des Benutzers nicht erkannt wurden.
- **Weiterleiten des Benutzers an die IVE-Standardanmeldeseite**  
wenn der Benutzer versucht, sich auf der Seite **RSA SecurID Authentication** auf einem Computer anzumelden, auf dem die SecurID-Software nicht installiert ist.
- **Auffordern des Benutzers, eine neue PIN zu erstellen (New PIN-Modus)**  
wenn der Benutzer sich erstmals bei Neoteris IVE anmeldet. (Dem Benutzer werden je nach verwendetem Anmeldeverfahren unterschiedliche Aufforderungen angezeigt. Bei Anmeldung über die Seite **RSA SecurID Authentication** werden die RSA-Aufforderungen zum Erstellen einer neuen PIN angezeigt. Andernfalls werden die IVE-Aufforderungen angezeigt.) Beachten Sie, dass der Benutzer für die erstmalige Anmeldung eine temporäre PIN benötigt.
- **Auffordern des Benutzers zur Eingabe des nächsten Tokens (Next Token-Modus)**  
wenn das vom Benutzer eingegebene Token nicht mit dem von ACE/Server erwarteten Token übereinstimmt. (Der Next Token-Modus ist für Benutzer transparent, die sich über die Seite **RSA SecurID Authentication** anmelden. Die RSA SecurID-Software übergibt das Token über das IVE und ohne Benutzerinteraktion an ACE/Server.)

Wenn der Benutzer die neue PIN oder das nächste Token eingibt (je nach Modus), bleiben drei Minuten für die Eingabe der erforderlichen Informationen. Danach bricht das IVE die Transaktion ab und fordert den Benutzer zur erneuten Eingabe der Anmeldeinformationen auf. Wenn die Anzahl der Versuche zur Benutzeranmeldung die zulässige Anzahl gleichzeitiger Transaktionen übersteigt, schlägt der Versuch fehl, der Benutzer wird zu einem erneuten Versuch aufgefordert, und es wird eine Meldung in das Systemprotokoll geschrieben.

Das IVE kann eine Höchstzahl von 200 gleichzeitigen Transaktionen (d. h. Verbindungen) mit ACE/Server verarbeiten. Der Neoteris IVE-Server initiiert eine Transaktion, wenn sich ein Benutzer beim Neoteris IVE anmeldet.

Das Neoteris IVE unterstützt die folgenden ACE/Server-Features: New PIN-Modus, Next Token-Modus, DES/SDI-Verschlüsselung, AES-Verschlüsselung, Unterstützung untergeordneter ACE/Server, Namenssperrungen und Clustering. Das IVE unterstützt über das RADIUS-Protokoll auch die New PIN- und Next Token-Modi von RSA SecurID.

---

**Hinweis:** Wegen der Einschränkungen der ACE/Server-Bibliothek unter UNIX können Sie u. U. nur eine ACE/Server-Konfiguration festlegen. Informationen zum Erzeugen einer ACE/Agent-Konfigurationsdatei für das IVE auf dem ACE-Server finden Sie unter „Generieren einer ACE/Agent-Konfigurationsdatei“ auf Seite 117.

---

Konfigurationsinformationen finden Sie unter „Festlegen einer ACE/Serverinstanz“ auf Seite 116.

## Netegrity SiteMinder-Server

Beim Authentifizieren von Benutzern mit einem Netegrity SiteMinder-Server können Sie den Neoteris IVE-Server für die Verwendung eines Netegrity SiteMinder-Servers für die Authentifizierung und Autorisierung bei Einzelanmeldungen konfigurieren. Das Neoteris IVE überprüft vor dem Gewähren des Zugriffs, ob der auf der Anmeldeseite eingegebene Benutzername und das Kennwort über den Netegrity SiteMinder-Server authentifiziert werden können. Wenn ein Benutzer über einen SiteMinder-Server mit einer bestimmten Schutzebene authentifiziert wird, erhält der Benutzer nahtlosen Zugriff auf Webressourcen mit einer Schutzebene, die geringer als die Schutzebene des Benutzers ist oder dieser entspricht. Wenn ein Benutzer versucht, auf eine Webressource mit einer höheren Schutzebene zuzugreifen, verarbeitet der Webserver, der die Ressource mit der höheren Schutzebene enthält, die erneute Authentifizierung der Anmeldeinformationen.

Bei Konfiguration mit einem SiteMinder-Authentifizierungsserver ermöglicht das IVE die Einzelanmeldung bei durch Netegrity geschützten Ressourcen, indem Netegrity SMSESSION-Cookies gespeichert und diese Cookies an anfordernde Webressourcen übergeben werden. Sie können folgende Aktionen ausführen:

- Erstellen von SMSESSION-Cookies mit dem benutzerdefinierten IVE-Web-Agenten (80)
- Abrufen von Netegrity SMSESSION-Cookies von einem Web-Agenten (81)
- Automatisches Anmelden beim IVE (81)

Konfigurationsinformationen finden Sie unter „Festlegen einer Netegrity SiteMinder-Instanz“ auf Seite 119.

## Erstellen von SMSESSION-Cookies mit dem benutzerdefinierten IVE-Web-Agenten

Über die Option **Authenticate using custom agent** verwendet das IVE einen benutzerdefinierten, mit dem Netegrity-SDK erstellten Web-Agenten. Bei einer Benutzeranmeldung beim IVE übergibt der benutzerdefinierte Web-Agent die Anmeldeinformationen des Benutzers an den SiteMinder-Richtlinienserver. Wenn die Anmeldeinformationen authentifiziert werden, erstellt der benutzerdefinierte Web-Agent ein SMSESSION-Cookie und speichert es im IVE. Beim Versuch des Benutzers, auf eine andere Webressource auf einem standardmäßigen Web-Agenten zuzugreifen, übergibt das IVE das Cookie zur Authentifizierung an den Web-Agenten.

Da das Netegrity SMSESSION-Cookie über das Netegrity-SDK erstellt wird, werden Cookies von Drittanbietern von anderen Web-Agenten nur akzeptiert, wenn sie auf das aktuelle Quarterly Maintenance Release (QMR) aktualisiert und zum Annehmen von Cookies von Drittanbietern konfiguriert wurden. Für SiteMinder, Version 4, verwenden Sie den QMR-Patch v4QMR4-010.zip, der auf der Netegrity-Website verfügbar ist. (Möglicherweise müssen Sie als Voraussetzung Hotfixes installieren, z. B. v4QMR4-windows.zip.) Für SiteMinder, Version 5, verwenden Sie den Hotfix QMR5 (erhältlich von Netegrity ab 30. September 2002).

Das Attribut **AcceptTPCookie** (Cookie von Drittanbietern akzeptieren) muss für den IIS-Webserver in der Konfigurationsdatei des Web-Agenten auf **yes** oder in der Windows-Registrierung auf **1** gesetzt sein. Der Speicherort dieses Attributs hängt von der verwendeten SiteMinder-Version und dem Webserver ab. Weitere Informationen finden Sie in der Dokumentation zu Ihrem SiteMinder-Server.

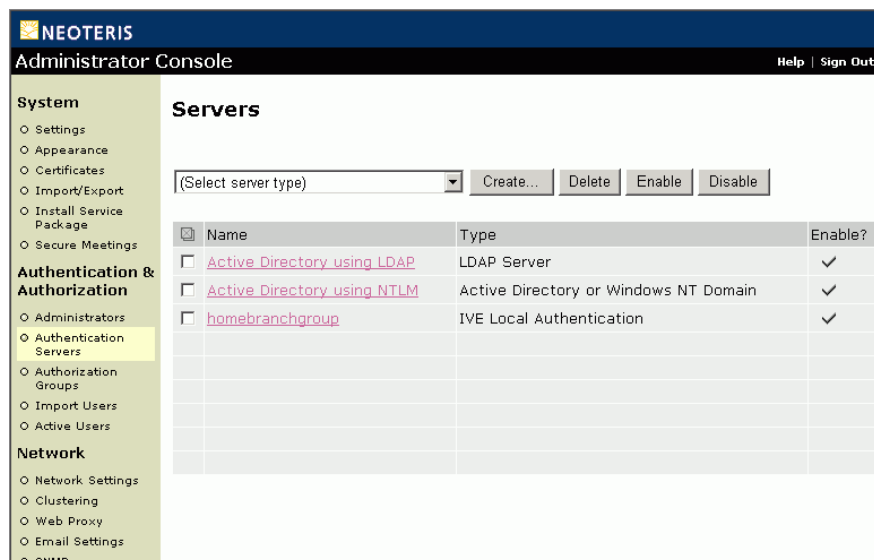


## Abrufen von Netegrity SMSESSION-Cookies von einem Web-Agenten

Mit der Option **Authenticate using HTML form post** erzeugt das IVE keine SMSESSION-Cookies, sondern ruft diese stattdessen von einem anderen Web-Agenten ab. Bei einer Benutzeranmeldung beim IVE stellt dieses eine Verbindung mit dem Web-Agenten her, der in der IVE-Administratorkonsole angegeben ist, und sendet an diesen die Anmeldeinformationen des Benutzers. Wenn die Anmeldeinformationen authentifiziert werden können, übergibt der Web-Agent ein SMSESSION-Cookie an das IVE, in dem es unter Verwendung des Netegrity-SDK überprüft und anschließend gespeichert wird. Beim Versuch des Benutzers, auf eine Webressource auf einem standardmäßigen Web-Agenten zuzugreifen, übergibt das IVE das Cookie zur Authentifizierung an den Web-Agenten.

## Automatisches Anmelden beim IVE

Wenn sich ein Benutzer bereits an einem anderen Netegrity-fähigen Server in der Domäne mit dem IVE angemeldet hat, ist über die Option **Automatic Sign in** der Zugriff auf das IVE ohne Aufforderung zur erneuten Anmeldung möglich. Das IVE überprüft lediglich anhand des Richtlinienservers das vom Browser des Benutzers gesendete SMSESSION-Cookie.



**Abbildung 36: Authentication & Authorization > Authentication Servers > Servers**

Sofern nicht anders angegeben, können Sie mehrere Instanzen eines Authentifizierungsservers erstellen. In der folgenden Abbildung wird eine Instanz für jeden unterstützten Server dargestellt.

## Authentication & Authorization > Menü „Administrators“

Auf den Registerkarten **Administrators** können Sie Administratorkonten erstellen und verwalten. Auf diesen Seiten können Sie folgende Aufgaben durchführen:

- Erstellen, Löschen, Bearbeiten und Suchen von Administratorengruppenkonten (82)
- Festlegen von Zeitbegrenzungen für Administratorengruppensitzungen (86)
- Festlegen von IP-Adresseinschränkungen für die Administratorengruppe (89)

### Registerkarte „Members“

#### ☒ Erstellen, Löschen, Bearbeiten und Suchen von Administratorengruppenkonten

Ein Administratorenkonto besteht aus einem Benutzernamen, dem vollständigen Namen und dem Authentifizierungstyp des Benutzers. Auf der Seite **Authentication & Authorization > Administrators > Members** sind die Administratorenkonten zusammengefasst. Hier können Sie Administratorenkonten erstellen, löschen, bearbeiten und suchen.

Das erste der Administratorengruppe hinzugefügte Administratorenkonto erstellen Sie über die Neoteris-Konsole, wenn das Initialisierungsskript für die Installation ausgeführt wird. Dieser Administrator wird automatisch für die Verwendung der lokalen Authentifizierung festgelegt. Wenn Sie den Neoteris IVE-Server für die Verwendung einer externen Benutzerdatenbank konfigurieren, können Sie weitere Administratoren erstellen, für deren Authentifizierung dieser externe Server verwendet wird.

---

**Hinweis:** Wenn Sie einem Endbenutzer beschränkte Verwaltungsrechte gewähren möchten, z. B. Hinzufügen von Benutzern zu einem Authentifizierungsserver, Löschen von Benutzern, Ändern der vollständigen Namen und Kennwörter von Benutzern, finden Sie entsprechende Informationen unter „Delegieren von Benutzerwaltungsrechten an Endbenutzer“ auf Seite 104.

---

## So erstellen Sie ein Administratorengruppenkonto

1. Wählen Sie in der Administratorkonsole die Registerkarte **Authentication & Authorization > Administrators > Members** aus.
2. Klicken Sie auf **New**, und geben Sie dann einen Benutzernamen und den vollständigen Namen des Administrators ein.
3. Wenn Sie den Benutzernamen eines Administrators nach dem Erstellen des Kontos ändern möchten, müssen Sie ein neues Konto erstellen.
4. Geben Sie den Authentifizierungstyp zur Überprüfung der Anmeldeinformationen des Benutzers an. Folgende Optionen sind möglich:
  - **Lokale Authentifizierung**—Geben Sie ein Kennwort für den Administrator ein. Der Neoteris IVE-Server vergleicht die Anmeldeinformationen des Benutzers mit dem angegebenen Benutzernamen und dem Kennwort.
  - **Externe Authentifizierung**—Stellen Sie sicher, dass auf dem angegebenen Authentifizierungsserver derselbe Benutzername vorhanden ist. Der Neoteris IVE-Server übergibt die Anmeldeinformationen des Benutzers zur Überprüfung an den Authentifizierungsserver. Wenn kein übereinstimmender Benutzername vorhanden ist, kann sich der Benutzer nicht anmelden.

---

**Hinweis:** Wenn Sie die **externe Authentifizierung** auswählen, muss der für die Administratorengruppe angegebene Server einen Datensatz für den betreffenden Benutzer enthalten. Weitere Informationen zum Angeben eines externen Servers für die Administratorengruppe finden Sie unter „Festlegen von IP-Adresseinschränkungen für die Administratorengruppe“ auf Seite 89.

---

5. Klicken Sie auf **Create User**. Der Administrator wird der Administratorengruppe hinzugefügt.

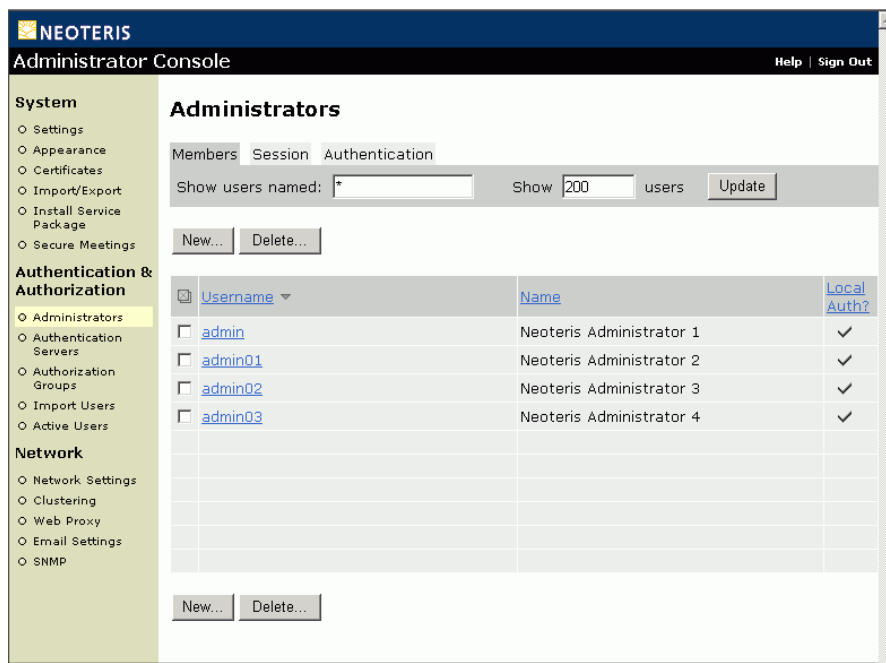


Abbildung 37: Authentication & Authorization > Administrators > Members

The screenshot shows the Neoteris Administrator Console interface. On the left is a navigation menu with categories: System, Authentication & Authorization, and Network. The 'Authentication & Authorization' section is expanded, showing sub-items like Administrators, Authentication Servers, Authorization Groups, Import Users, and Active Users. The main content area is titled 'New Administrator'. It displays 'Current # of local users: 4'. There are input fields for 'Username:' (containing 'Admin04') and 'Full Name:' (containing 'Administrator 4'). Below these is a section titled 'Neoteris Authentication Type' with two radio buttons: 'Local authentication' (selected) and 'External authentication'. Under 'Local authentication' are fields for 'Password:' and 'Confirm Password:', both masked with asterisks. A note under 'External authentication' states: 'If there is no external server, this user will NOT be able to sign in. Use local authentication unless external authentication will be enabled later.' At the bottom of the form is a 'Create User' button.

Abbildung 38: Authentication & Authorization > Administrators > Members > New...

## Zusätzliche Aufgaben

- Um ein Administratorengruppenkonto zu löschen, markieren Sie die zu löschenden Konten, und klicken Sie dann auf **Delete**. Die Konten werden sofort gelöscht.
- Um ein Administratorengruppenkonto zu bearbeiten, klicken Sie auf den Benutzernamen des Benutzers, dessen Konto Sie bearbeiten möchten. Sie können den vollständigen Namen des Benutzers bearbeiten, die Gruppenmitgliedschaft des Benutzers ändern oder den Authentifizierungstyp des Benutzers ändern. Wenn Sie für die Administratorengruppe keinen externen Authentifizierungsserver angeben (siehe „Festlegen von IP-Adresseinschränkungen für die Administratorengruppe“ auf Seite 89), müssen Sie die **lokale Authentifizierung** auswählen und ein Benutzerkennwort festlegen, das in der lokalen Datenbank gespeichert und zum Authentifizieren des Benutzers verwendet wird. Klicken Sie abschließend auf **Save Changes**.

---

**Hinweis:** Sie können einen Benutzernamen nicht ändern. Wenn Sie den Benutzernamen eines Administrators nach dem Erstellen des Kontos ändern möchten, müssen Sie für diesen Administrator ein neues Konto erstellen.

---

- Geben Sie zum Suchen von Administratorengruppenkonten im Feld **Show users named** den Namen des zu suchenden Benutzers ein. Geben Sie im Feld **Show \_ users** eine Zahl ein, um die Anzahl der angezeigten Ergebnisse einzuschränken. Klicken Sie zum Anzeigen der Suchergebnisse auf **Update**. Wenn keine Namen angezeigt werden, ist kein mit den Suchkriterien übereinstimmendes Administratorengruppenkonto vorhanden.

**Hinweis:**

- Im Feld **Show users named** können Sie als Platzhalter ein Sternchen (\*) verwenden, wobei das \* für eine beliebige Anzahl von Zeichen steht. Wenn Sie z. B. nach allen Benutzernamen suchen möchten, die die Buchstaben `admin` enthalten, geben Sie im Feld **Show users named** die Zeichenfolge `*admin*` ein. Bei der Suche muss die Groß- und Kleinschreibung beachtet werden.
- Wenn Sie die gesamte Liste von Administratorengruppenkonten erneut anzeigen möchten, geben Sie im Feld **Show users named** ein \* ein, oder löschen Sie dessen Inhalt, und klicken Sie dann auf **Update**.

## Registerkarte „Session“

### ☒ Festlegen von Zeitbegrenzungen für Administratorengruppensitzungen

Die Standardzeitbegrenzung für eine Administratorsitzung beträgt dreißig Minuten. Nach dieser Zeitspanne wird die Sitzung geschlossen und das Ereignis im Systemprotokoll protokolliert. Zusätzlich ist ein Wert für Leerlaufzeiten von Sitzungen von fünf Minuten festgelegt. Dies bedeutet, dass die Administratorsitzung geschlossen und im Systemprotokoll ein Ereignis protokolliert wird, wenn sie für fünf Minuten inaktiv ist. In jedem Fall muss sich der Administrator zur Wiederaufnahme der Arbeit neu anmelden. Diese Werte können auf der Seite **Group > Administrators > Session** geändert werden.

#### So legen Sie Zeitbegrenzungen für Administratorengruppensitzungen fest

1. Wählen Sie in der Administratorkonsole das Menü **Authentication & Authorization > Administrators** aus.
2. Wählen Sie auf den Gruppenregisterkarten die Option **Session** aus.
3. Geben Sie die Anzahl der Minuten an, die sich eine Administratorsitzung im Leerlauf befinden kann, bevor sie beendet wird. Die Mindestzeit beträgt drei Minuten.

4. Geben Sie die Anzahl der Minuten an, die eine aktive Administratorsitzung geöffnet bleiben kann, bevor sie beendet wird. Die Mindestzeit beträgt drei Minuten.
5. Klicken Sie auf **Save Changes**.

The screenshot shows the Neoteris Administrator Console interface. The left sidebar contains a navigation menu with categories: System, Authentication & Authorization, and Network. Under Authentication & Authorization, 'Administrators' is selected. The main content area is titled 'Administrators' and has three tabs: 'Members', 'Session', and 'Authentication'. The 'Session' tab is active, showing 'Session timeout' settings. 'Idle Timeout' is set to 180 minutes and 'Max. Session Length' is set to 360 minutes. Below this is the 'Enable roaming session' section, which includes a warning about session cookies and three radio button options: 'Enabled (maximize mobility)' (selected), 'Limited to subnet range (minimum mobility, increased security)', and 'Disabled (maximize security)'. The 'Limited to subnet range' option has a 'Netmask' input field.

Abbildung 39: Authentication & Authorization > Administrators > Session

## Authentication > Unterregisterkarte „Authentication Server“

### ☒ Festlegen eines Servers für die Authentifizierung der Administratorengruppe

Auf dieser Registerkarte können Sie einen externen Server für die Authentifizierung von Mitgliedern der Administratorengruppe angeben. Beachten Sie, dass sich Administratoren bei aktivierter DMZ-Funktion nur dann von außerhalb anmelden können, wenn Sie diese Option explizit aktivieren. Wenn Sie keinen externen Server angeben, müssen Sie für jedes Mitglied der Administratorengruppe ein Kennwort festlegen. Weitere Informationen erhalten Sie unter „Erstellen, Löschen, Bearbeiten und Suchen von Administratorengruppenkonten“ auf Seite 82.

## So legen Sie einen Server für die Authentifizierung der Administratorengruppe fest

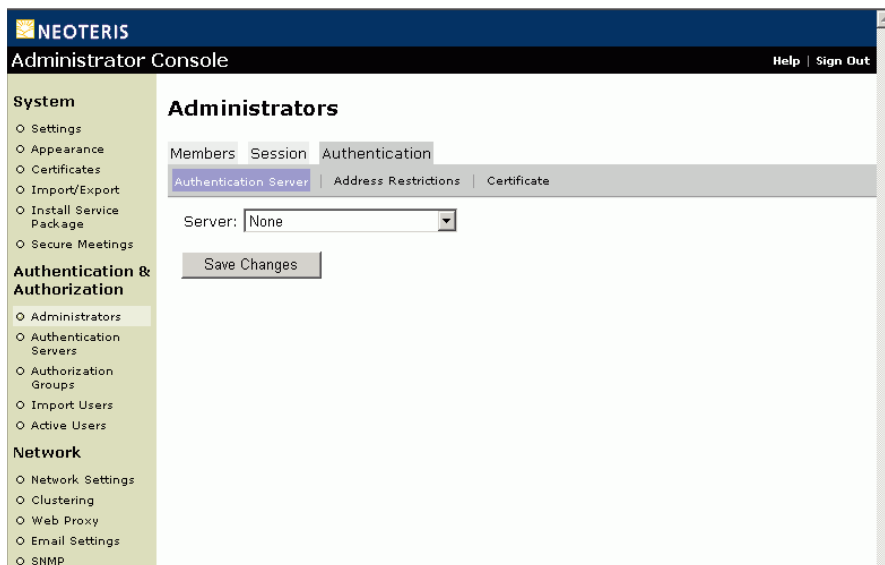
1. Wählen Sie in der Administratorkonsole die Registerkarte **Authentication & Authorization > Administrators > Authentication Server** aus.
2. Wählen Sie die Authentifizierungsinstanz zum Authentifizieren von Mitgliedern der Administratorengruppe aus. Informationen zum Konfigurieren einer Authentifizierungsinstanz finden Sie unter „Definieren einer Authentifizierungsserverinstanz“ auf Seite 92.

Wenn Sie nur die lokale Authentifizierung verwenden möchten, wählen Sie im Dropdownmenü **Server** die Option **None** aus. Für jedes Administratorenkonto müssen Sie die Verwendung der lokalen Authentifizierung angeben sowie ein Benutzerkennwort festlegen. Weitere Informationen finden Sie unter „Erstellen, Löschen, Bearbeiten und Suchen von Administratorengruppenkonten“ auf Seite 82.

---

**Hinweis:** Sie können nur eine Authentifizierungsinstanz zum Authentifizieren von Mitgliedern der Administratorengruppe angeben. Wenn Sie Administratorenkonten für Benutzer erstellen möchten, für die auf diesem externen Server keine Datensätze vorhanden sind, konfigurieren Sie einfach deren Benutzerkonten für die Verwendung der lokalen Authentifizierung.

---



**Abbildung 40:** Authentication & Authorization > Administrators > Authentication > Authentication Server



## Authentication > Unterregisterkarte „Address Restrictions“

### ☒ Festlegen von IP-Adresseinschränkungen für die Administratorengruppe

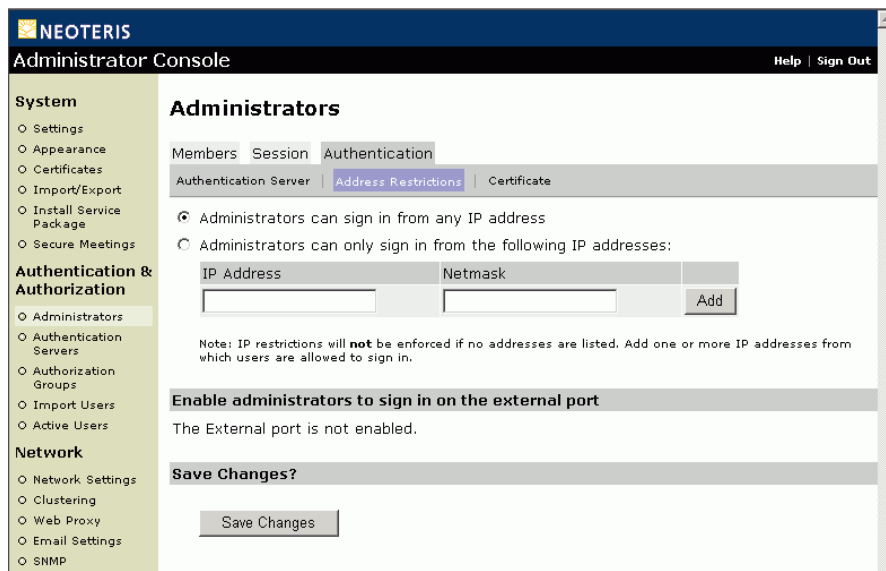
Auf dieser Registerkarte können Sie den Administratorzugriff auf den Neoteris IVE-Server auf bestimmte IP-Adressen einschränken.

#### So legen Sie Adresseinschränkungen für die Administratorengruppe fest

1. Wählen Sie in der Administratorkonsole die Registerkarte **Authentication & Authorization > Administrators > Address Restrictions** aus.
2. Geben Sie an, ob die Anmeldung für Administratoren von einem beliebigen Ort oder nur von bestimmten IP-Adressen aus möglich sein soll. Wenn Sie die zweite Option auswählen, müssen Sie die entsprechenden IP-Adressen angeben. Andernfalls können sich Benutzer von beliebigen Orten aus anmelden.

Unter **Administrator login on External Port** werden Aktivierungs-/Deaktivierungsoptionen oder die Meldung „The External port is not enabled“ angezeigt. In der folgenden Liste werden die möglichen Aktionen zum Zulassen bzw. Verweigern der Administratoranmeldung über den externen Port erläutert.

- Wenn der externe Port nicht aktiviert ist und Sie die Administratoranmeldung über den externen Port zulassen möchten, wechseln Sie zu **Network Settings > External Port**, und aktualisieren Sie die Einstellung wie unter „Aktivieren des externen Ports (DMZ-Schnittstelle)“ auf Seite 241 beschrieben.
  - Wenn der externe Port aktiviert ist und Administratoren sich nur über den internen Port anmelden sollen, klicken Sie auf **Disable**. Dies ist die Standardeinstellung.
  - Wenn der externe Port aktiviert ist und Administratoren sich über den internen oder über den externen Port anmelden sollen, klicken Sie auf **Enable**.
3. Wählen Sie das Untermenü **Certificate** aus. Geben Sie an, ob Administratoren für die Authentifizierung über ein clientseitiges Zertifikat verfügen müssen. Sie können außerdem ein Attribut-Wert-Paar angeben, das für die Authentifizierung erforderlich ist.
  4. Klicken Sie auf **Save Changes**.



**Abbildung 41: Authentication & Authorization > Administrators > Address Restrictions**

## Authentication > Unterregisterkarte „Certificate“

### ☑ Angeben von Zertifikatanforderungen für die Administratorengruppe

Auf dieser Registerkarte können Sie angeben, ob sich Administratoren von einem Computer mit einem clientseitigen Zertifikat anmelden müssen.

#### So geben Sie Zertifikatanforderungen für die Administratorengruppe an

1. Wählen Sie in der Administratorkonsole die Registerkarte **Authentication & Authorization > Administrators > Certificate** aus.
2. Geben Sie an, ob Administratoren für die Authentifizierung über ein clientseitiges Zertifikat verfügen müssen. Sie können außerdem ein Attribut-Wert-Paar angeben, das für die Authentifizierung erforderlich ist.
3. Klicken Sie auf **Save Changes**.

The screenshot shows the Neoteris Administrator Console interface. The left sidebar contains a navigation menu with categories: System, Authentication & Authorization, and Network. The 'Authentication & Authorization' section is expanded, showing 'Administrators' as the selected item. The main content area is titled 'Administrators' and has three tabs: 'Members', 'Session', and 'Authentication'. The 'Authentication' tab is active, and within it, the 'Certificate' sub-tab is selected. The 'Certificate' sub-tab contains the 'SSL Client-side Digital Certificate Authentication' section. This section has two radio button options: 'Administrators do NOT require clientside certificate for authentication' (which is selected) and 'Administrators require clientside certificate with following attributes for authentication:'. Below the second option is a table with two columns: 'Certificate Field' and 'Field Value'. There is an 'Add' button to the right of the table. Below the table, a note states: 'Certificate Field is a component of a X.509 Distinguished Name: C, ST, L, O, OU, CN, T, I, G, S, D, UID, or Email. Both Certificate Field and its value are case insensitive.' At the bottom of the page, there is a 'Save Changes?' section with a 'Save Changes' button.

NEOTERIS

Administrator Console Help | Sign Out

**System**

- Settings
- Appearance
- Certificates
- Import/Export
- Install Service Package
- Secure Meetings

**Authentication & Authorization**

- Administrators
- Authentication Servers
- Authorization Groups
- Import Users
- Active Users

**Network**

- Network Settings
- Clustering
- Web Proxy
- Email Settings
- SNMP

**Administrators**

Members Session Authentication

Authentication Server Address Restrictions Certificate

**SSL Client-side Digital Certificate Authentication**

☒ Administrators do NOT require clientside certificate for authentication

☐ Administrators require clientside certificate with following attributes for authentication:

Certificate Field	Field Value
<input type="text"/>	<input type="text"/>

Add

Certificate Field is a component of a X.509 Distinguished Name: C, ST, L, O, OU, CN, T, I, G, S, D, UID, or Email. Both Certificate Field and its value are case insensitive.

**Save Changes?**

Save Changes

Abbildung 42: Authentication & Authorization > Administrators > Certificate

## Authentication & Authorization > Menü „Authentication Servers“

Dieser Abschnitt enthält Anweisungen zum Festlegen einer Authentifizierungsserverinstanz (Seite 92) und zum Delegieren von Benutzerverwaltungsrechten an Endbenutzer (Seite 104).

### ☒ Definieren einer Authentifizierungsserverinstanz

Zum Festlegen einer Authentifizierungsserverinstanz sind folgende Schritte erforderlich:

- 1 Festlegen der Servereinstellungen, einschließlich der Serverinformationen und der Art der Zuordnungen von Benutzern zu Gruppen durch das IVE.
- 2 Angeben der Gruppenzuordnungsinformationen für die Instanz.

Bei der Konfiguration des lokalen IVE-Authentifizierungsservers:

- 3 Definieren lokaler Benutzerkonten.

### Schritt 1: Angeben von Serverinformationen und der Option für die Zuordnung von Benutzern zu Gruppen

1. Wählen Sie in der Administratorkonsole das Menü **Authentication & Authorization > Authentication Servers** (Seite 81) aus.
2. Wählen Sie in der Dropdownliste den Typ des Authentifizierungsservers aus, für den Sie eine Instanz definieren möchten.

#### Hinweis:

- Zum Authentifizieren von Active Directory können Sie das NTLM- und das LDAP-Protokoll verwenden. Sie können den Active Directory-Server mit folgenden Protokollen authentifizieren:
  - **NTLM**—Wählen Sie **Active Directory or Windows NT Domain** (siehe Seite 95) aus
  - **LDAP**—Wählen Sie **LDAP Server** (siehe Seite 96) aus

- Wenn Sie zum Authentifizieren von Benutzeradministratoren eine Serverinstanz erstellen, müssen Sie **IVE Local Authentication** auswählen.
3. Klicken Sie auf **Create**. Die Konfigurationsseite für den ausgewählten Server wird angezeigt.

---

**Hinweis:** Übersichtsinformationen zu unterstützten Servertypen finden Sie unter „Unterstützte Authentifizierungsserver“ auf Seite 75.

---

4. Geben Sie einen Namen ein, um die Serverinstanz zu bezeichnen. Da Benutzern das Prinzip der Anmeldung bei einem Authentifizierungsserver nicht notwendigerweise sofort vertraut ist, wird die Verwendung eines bekannten Namens für die Gruppe empfohlen, zu der der betreffende Benutzer gehört, z. B. „Firma“ oder „Hauptniederlassung“.
5. Geben Sie die für die Herstellung der Verbindung mit dem Server erforderlichen Informationen ein. Details zum ausgewählten Server finden Sie im entsprechenden Abschnitt:
  - Definieren einer Active Directory-Serverinstanz oder einer Windows NT-Domänenserverinstanz (106)
  - Festlegen einer LDAP-Serverinstanz (108)
  - Festlegen einer NIS-Serverinstanz (112)
  - Festlegen einer NIS-Serverinstanz (112)
  - Festlegen einer RADIUS-Serverinstanz (113)
  - Festlegen einer ACE/Serverinstanz (116)
  - Festlegen einer Netegrity SiteMinder-Instanz (119)

---

**Hinweis:** Wenn Sie ACE/Server für die Authentifizierung verwenden, müssen Sie eine ACE/Agent-Konfigurationsdatei (**sdconf.rec**) für das IVE auf dem ACE-Server generieren. Entsprechende Anweisungen finden Sie unter „Generieren einer ACE/Agent-Konfigurationsdatei“ auf Seite 117.

---

6. Geben Sie im Abschnitt **Authorization Group Settings** an, wie die Zuordnung von Benutzern zu Gruppen durch das IVE erfolgen soll, indem Sie eine der folgenden Optionen auswählen:
  - **Authorization group assigned based on attribute in authentication response**  
*Diese Option ist nur verfügbar, wenn Sie in der Dropdownliste in Schritt 2 die Option **LDAP Server** oder **Radius Server** auswählen.*  
Wählen Sie diese Option aus, wenn das IVE Benutzer Autorisierungsgruppen auf Grundlage der Gruppeninformationen zuordnen soll, die von LDAP oder RADIUS zurückgegeben werden. Wenn Sie z. B. einen Active Directory-Server konfigurieren, der zur Authentifizierung das LDAP-Protokoll verwendet, geben Sie im Feld **Group Attribute** das Attribut **memberof** ein. Das IVE vergleicht die für dieses Attribut zurückgegebenen Daten mit den Regeln für die Zuordnung von Benutzern zu Gruppen, die Sie auf der Registerkarte **Group Mapping** erstellt haben.

- **Authorization group assigned based on querying a group lookup server**

*Diese Option ist mit Ausnahme des lokalen IVE-Authentifizierungsservers für alle Server verfügbar.*

Wählen Sie diese Option aus, wenn das IVE Benutzer Autorisierungsgruppen auf Grundlage der Gruppeninformationen zuordnen soll, die von einem LDAP-Server zurückgegeben werden. Wenn Sie diese Option für eine LDAP-Serverinstanz auswählen, authentifiziert das IVE Benutzer mit dem Server, der für die Serverinstanz festgelegt ist, und autorisiert Benutzer dann mit dem zusätzlichen LDAP-Server, den Sie im Dialogfeld **Configure Group Lookup Server** (Seite 97) festlegen.

---

**Wichtig:** Wenn Sie diese Option für Autorisierungsgruppeneinstellungen auswählen, klicken Sie auf die Schaltfläche **Define**, um auf das Konfigurationsdialogfeld für Gruppenlookupserver zuzugreifen. Weitere Informationen erhalten Sie unter „Konfigurieren eines Servers für das Gruppenlookup“ auf Seite 97.

---

- **Authorization group assigned based on username**

Diese Option ist für alle Server verfügbar. Wählen Sie diese Option aus, wenn Benutzer auf Grundlage des Benutzernamens Autorisierungsgruppen zugeordnet werden sollen.

- **All users are assigned to ...**

Diese Option ist für alle Server verfügbar. Wählen Sie diese Option aus, wenn das IVE *alle* authentifizierten Benutzer der angegebenen Autorisierungsgruppe zuordnen soll.

7. Klicken Sie auf **Save Changes**, um Schritt 1 abzuschließen. Die Registerkarten **Group Mapping** und **User** werden angezeigt.
8. Wechseln Sie zu „Schritt 2: Angeben von Informationen für die Gruppenzuordnung“ auf Seite 98.

**NEOTERIS**  
Administrator Console Help | Sign Out

**System**

- Settings
- Appearance
- Certificates
- Import/Export
- Install Service Package
- Secure Meetings

**Authentication & Authorization**

- Administrators
- Authentication Servers
- Authorization Groups
- Import Users
- Active Users

**Network**

- Network Settings
- Clustering
- Web Proxy
- Email Settings
- SNMP

[Authentication Servers >](#)  
**New NT Server**

Name:  Label to reference this server

Primary Domain Controller or Active Directory:  Name or IP address

Backup Domain Controller or Active Directory:  Name or IP address

Domain:  NT domain name

**Authorization Group Settings**

Specify how users will be mapped to authorization groups:

☒ **Authorization group assigned based on querying a group lookup server**

Server Properties: 

Type: Generic  
Server: 192.168.217.100  
Port: 389  
Connection: Unencrypted  
Filter: sAMAccountname=<USER>

☐ Authorization group assigned based on username

☐ All users are assigned to:

Authorization Group:

#### Abbildung 43: Konfigurieren eines Active Directory-Servers, der NTLM verwendet

Wenn Sie einen Active Directory-Server konfigurieren, der für die Authentifizierung das NTLM-Protokoll verwendet, und Sie für das Gruppenlookup (Autorisierung) denselben AD-Server verwenden möchten, müssen Sie das Dialogfeld für Gruppenlookupserver konfigurieren (siehe Seite 97). In der folgenden Abbildung (43) wird die Serverkonfigurationsseite nach dem Festlegen der LDAP-Attribute im Dialogfeld für Gruppenlookupserver dargestellt.

NEOTERIS

Administrator Console

Help | Sign Out

System

- Settings
- Appearance
- Certificates
- Import/Export
- Install Service Package
- Secure Meetings

Authentication & Authorization

- Administrators
- Authentication Servers
- Authorization Groups
- Import Users
- Active Users

Network

- Network Settings
- Clustering
- Web Proxy
- Email Settings
- SNMP

Authentication Servers >

New LDAP Server

Name:

Active Directory using LDAP

Label to reference this server

LDAP Server:

192.168.217.100

Name or IP address

LDAP Port:

389

Backup LDAP Server1:

Name or IP address

Backup LDAP Port1:

Backup LDAP Server2:

Name or IP address

Backup LDAP Port2:

Connection:

☒ Unencrypted
 ☐ LDAPS
 ☐ LDAP over TLS

Test Connection

Static Distinguished Name (DN)

Directly access a user's DN. Enter the complete DN path, including <USER> to search for the username entered on the Sign-In page.

DN:

example: cn=<USER>,dc=sales,dc=com

Dynamic Distinguished Name (DN)

Begin searching at a specified base. Enter the path to the base at which you want to begin the search. Specify a filter to fine-tune the search, including <USER> to search for the username entered on the Sign-In page.

Base DN:

dc=demo,dc=danastreet,dc=net

example: dc=sales,dc=com

Filter:

MAccountname=<USER>

example: cn=<USER>

☐ Require application (Neoteris IVE) authentication to search the LDAP database

Application DN:

Application password:

Authorization Group Settings

Specify how users will be mapped to authorization groups:

☒ Authorization group assigned based on attribute in authentication response

Group Attribute:

memberof

Name of the relevant attribute in the authentication response

☐ Authorization group assigned based on querying a group lookup server

**Abbildung 44: Konfigurieren eines Active Directory-Servers, der LDAP verwendet**  
Wenn Sie einen Active Directory-Server konfigurieren, der für die Authentifizierung das LDAP-Protokoll verwendet, und Sie für das Gruppenlookup (Autorisierung) denselben AD-Server verwenden möchten, müssen Sie lediglich die Informationen für das Gruppenlookup auf der Serverkonfigurationsseite konfigurieren.



## ☑ Konfigurieren eines Servers für das Gruppenlookup

Mit einem LDAP-Server können Sie die Autorisierung für alle Authentifizierungsserver durchführen. Wenn Sie die Option **Authorization group assigned based on querying a group lookup server** auswählen (Seite 94), müssen Sie die Serverinformationen für den LDAP-Gruppenlookupserver angeben.

---

**Hinweis:** Wenn Sie diese Option für eine LDAP-Serverinstanz auswählen, authentifiziert das IVE Benutzer mit dem für die Serverinstanz festgelegten Server und autorisiert Benutzer dann unter Verwendung des Servers, der im Dialogfeld **Configure Group Lookup Server** (Seite 98) angegeben ist. Der für die Authentifizierung und der für die Autorisierung angegebene Server können identisch sein. Im Falle eines Active Directory-Servers zum Beispiel, der zur Authentifizierung NTLM verwendet, können Sie für die Autorisierung im Dialogfeld für den Gruppenlookupserver denselben AD-Server angeben.

---

### So konfigurieren Sie einen Server für das Gruppenlookup

1. Führen Sie auf der Konfigurationsseite für den Authentifizierungsserver unter **Authorization Group Settings** Folgendes aus:
  - 1 Wählen Sie die Option **Authorization group assigned based on querying a group lookup server** aus.
  - 2 Klicken Sie auf die Schaltfläche **Define**.
2. Geben Sie in der Dropdownliste **LDAP Server Type** Folgendes an:
  - **Look Up Group**  
Wählen Sie diese Option, um ein standardisiertes Gruppenlookup durchzuführen, z. B. mit einem Active Directory-Server.
  - **Look Up User Then Group**  
Wählen Sie diese Option, wenn Sie zusätzliche Benutzer- und Gruppenfilter festlegen müssen, z. B. mit einem iPlanet-Server.
3. Geben Sie die Einstellungen für den LDAP-Server ein, und klicken Sie dann auf **OK**.

**Abbildung 45: Dialogfeld für die Konfiguration des Gruppenlookupservers—  
„Look Up Group“**

## Schritt 2: Angeben von Informationen für die Gruppenzuordnung

1. Klicken Sie für die in Schritt 1 konfigurierte Instanz auf die Registerkarte **Group Mapping**.

Wenn Sie Benutzer IVE-Autorisierungsgruppen nach Gruppeninformationen zuordnen möchten, die als Teil der Authentifizierungsantwort zurückgegeben oder durch eine Abfrage an den Gruppenlookupserver abgerufen wurden, gehen Sie wie folgt vor:

1. Geben Sie im Feld **Rule 1** die Gruppennamen ein, die von dem Authentifizierungsserver zurückgegeben werden können, den Sie **einer** IVE-Autorisierungsgruppe zuordnen möchten. Geben Sie pro Zeile eine externe Gruppe (Authentifizierungsserver) ein.
2. Wählen Sie die IVE-Authentifizierungsgruppe aus, der alle authentifizierten Benutzer zugeordnet werden, die Regel 1 entsprechen.
3. Erstellen Sie weitere Regeln zum Behandeln externer Gruppen, die Sie verschiedenen IVE-Autorisierungsgruppen zuordnen möchten.

In **Abbildung 46** auf Seite 100 finden Sie ein Beispiel für das Erstellen von Regeln für die Zuordnung von Benutzern zu Gruppen bei Verwendung von LDAP-Attributen.

Wenn Sie Benutzer IVE-Autorisierungsgruppen nach Benutzernamen zuordnen möchten, führen Sie die folgenden Schritte aus:

- 1 Geben Sie im Feld **Rule 1** die Benutzernamen ein, die Sie **einer** IVE-Autorisierungsgruppe zuordnen möchten. Geben Sie pro Zeile einen Benutzernamen ein.
- 2 Wählen Sie die IVE-Authentifizierungsgruppe aus, der alle authentifizierten Benutzer zugeordnet werden, die Regel 1 entsprechen.
- 3 Erstellen Sie weitere Regeln zum Behandeln von Benutzernamen, die Sie verschiedenen IVE-Autorisierungsgruppen zuordnen möchten.

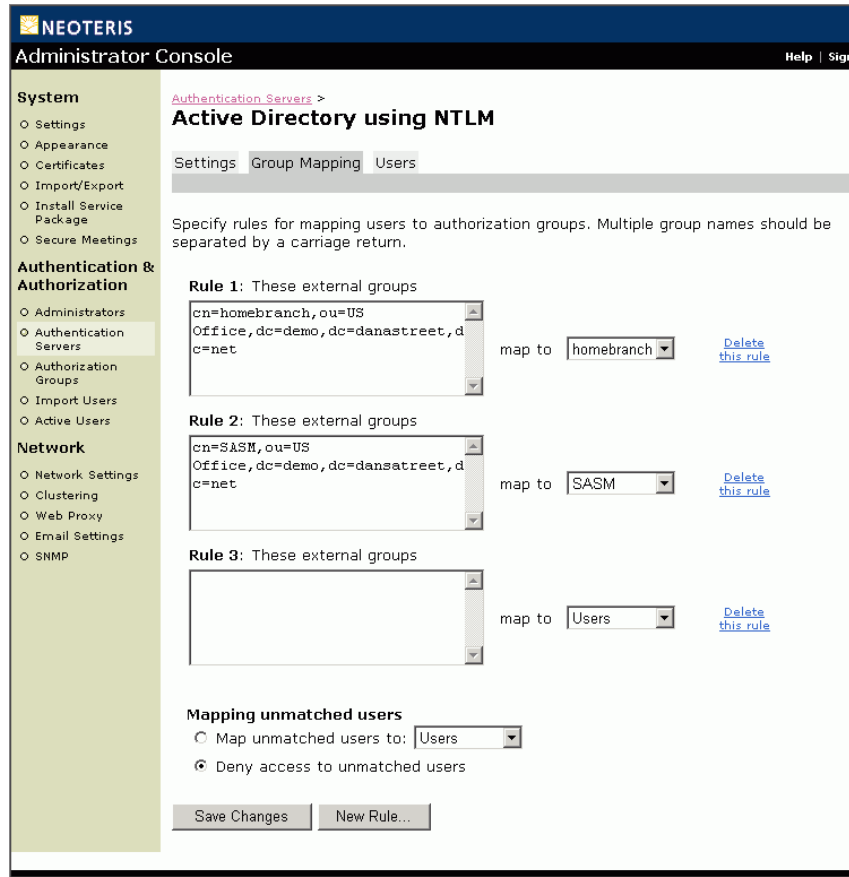
---

**Wichtig:** In IVE, Version 3.0, können Benutzer pro Sitzung jeweils nur einer Autorisierungsgruppe zugeordnet werden. Wenn z. B. ein LDAP- oder ein RADIUS-Benutzer in mehreren Gruppen vorhanden ist, beispielsweise in „Marketing“, „Entwicklung“ und „Firma“, müssen Sie für die Behandlung jeder Gruppe mehrere Instanzen des Authentifizierungsservers einrichten. Bei der Anmeldung des Benutzers beim IVE muss er die Authentifizierungsserverinstanz angeben, die der Gruppe entspricht, der er für die Sitzung beitreten möchte.

---

2. Geben Sie unter **Mapping unmatched users** an, ob Benutzer, auf die keine Regel zutrifft, einer bestimmten Gruppe zugeordnet oder ihnen der Zugriff verweigert werden soll.
3. Klicken Sie abschließend auf **Save Changes**.

Wenn Sie eine lokale IVE-Authentifizierungsserverinstanz erstellt haben, fahren Sie mit „Schritt 3: Erstellen lokaler Benutzer (nur bei lokaler IVE-Authentifizierung)“ auf Seite 101 fort. Wenn Sie eine externe Serverinstanz erstellt haben, ist dieses Verfahren abgeschlossen. Sofern dies nicht bereits erfolgt ist, konfigurieren Sie die Autorisierungsgruppen, denen für diese Instanz Benutzer zugeordnet werden. Weitere Informationen finden Sie unter „Übersicht über Authentifizierung und Autorisierung“ auf Seite 72.



**Abbildung 46: Konfigurieren der Registerkarte „Group Mapping“**

In diesem Beispiel wird die Verwendung von LDAP-Attributen zum Erstellen von Regeln für die Zuordnung von Benutzern zu Gruppen dargestellt. Beachten Sie, dass Sie unabhängig vom Abrufverfahren für die Gruppeninformationen (als Teil der Authentifizierungsantwort oder durch Abfrage an den Gruppenlookupserver) dieselben Attribute für die Benutzer-zu-Gruppen-Zuordnungsregeln verwenden.

### Schritt 3: Erstellen lokaler Benutzer (nur bei lokaler IVE-Authentifizierung)

Wenn Sie als Typ des Authentifizierungsservers „IVE local authentication“ auswählen, müssen Sie für diese Datenbank lokale Benutzerdatensätze definieren. Lokale Benutzerdatensätze bestehen aus einem Benutzernamen, dem vollständigen Namen und dem Kennwort des Benutzers. In einer lokalen Datenbank gespeicherte Benutzer müssen diese Datenbank zur Authentifizierung auf der IVE-Anmeldeseite angeben. Sie können lokale Benutzerdatensätze für Benutzer erstellen, die normalerweise von einem externen Authentifizierungsserver überprüft werden, den Sie deaktivieren möchten. Dies bietet sich auch an, wenn Sie schnell eine Gruppe von temporären Benutzern erstellen möchten.

#### So erstellen Sie lokale Benutzerdatensätze für die lokale IVE-Authentifizierung

1. Klicken Sie für die in Schritt 1 erstellte Datenbank auf die Registerkarte **Local Users**.
2. Klicken Sie auf der Seite **Local Users** auf **New**.
3. Geben Sie den Benutzernamen, den vollständigen Namen des Benutzers und ein Kennwort ein.

Hinweis:

- In Benutzernamen darf die Zeichenkombination „~“ nicht enthalten sein.
  - Wenn Sie den Benutzernamen eines Benutzers nach dem Erstellen seines Kontos ändern möchten, müssen Sie ein neues Konto erstellen.
4. Klicken Sie auf **Save Changes**. Der Benutzerdatensatz wird der IVE-Datenbank hinzugefügt. Informationen zum Löschen, Bearbeiten und Suchen eines Benutzerdatensatzes finden Sie unter Seite 102-103.

The screenshot shows the NEOTERIS Administrator Console interface. On the left is a navigation menu with categories: System (Settings, Appearance, Certificates, Import/Export, Install Service Package, Secure Meetings) and Authentication & Authorization (Administrators, Authentication Servers, Authorization Groups, Import Users, Active Users). The 'Authentication Servers' link is highlighted. The main content area is titled 'New Local User' and contains the following fields: Username (ken), Fullname (Kenneth Spalding), Authenticate using (homebranchgroup), Password (masked with asterisks), and Confirm Password (masked with asterisks). A 'Save Changes' button is at the bottom.

**Abbildung 47: Authentication & Authorization > Authorization Groups > New Local User**

### So verwalten Sie ein lokales Benutzerkonto

1. Wählen Sie in der Administratorkonsole das Menü **Authentication & Authorization > Authentication Servers** aus.
2. Wählen Sie die IVE-Serverinstanz aus, zu der der Benutzer gehört, und klicken Sie auf die Registerkarte **Users**.
3. Führen Sie eine der folgenden Aufgaben durch:
  - Um einen lokalen Benutzerdatensatz zu löschen, markieren Sie den zu löschenden Datensatz, und klicken Sie dann auf **Delete**. Der Datensatz wird sofort gelöscht.
  - Um einen lokalen Benutzerdatensatz zu bearbeiten, klicken Sie auf das Benutzerkonto, das Sie bearbeiten möchten. Gehen Sie auf der Zusammenfassungsseite für Konten wie folgt vor:
    - 1 Bearbeiten Sie den vollständigen Namen des Benutzers, oder ändern Sie das Kennwort des Benutzers.
    - 2 Klicken Sie auf **Save Changes**.

---

**Hinweis:** Sie können einen Benutzernamen nicht ändern. Wenn Sie den Benutzernamen eines Benutzers nach dem Erstellen seines Kontos ändern möchten, müssen Sie ein neues Konto für diesen Benutzer erstellen.

---

## So suchen Sie einen lokalen Benutzerdatensatz

1. Wählen Sie in der Administratorkonsole das Menü **Authentication & Authorization > Authentication Servers** aus.
2. Wählen Sie die IVE-Serverinstanz aus, zu der der Benutzer gehört, und klicken Sie auf die Registerkarte **Local Users**.
3. Geben Sie im Feld **Show users named** den Namen des zu suchenden Benutzers ein. Geben Sie im Feld **Show \_ users** eine Zahl ein, um die Anzahl der angezeigten Ergebnisse einzuschränken. Klicken Sie zum Anzeigen der Suchergebnisse auf **Update**. Wenn keine Namen angezeigt werden, ist kein mit den Suchkriterien übereinstimmendes Konto vorhanden.

Hinweis:

- Im Feld **Show users named** können Sie als Platzhalter ein Sternchen (\*) verwenden, wobei das \* für eine beliebige Anzahl von Zeichen steht. Wenn Sie z. B. alle Benutzernamen suchen möchten, die die Buchstaben dave enthalten, geben Sie im Feld **Show users named** die Zeichenfolge \*dave\* ein. Bei der Suche muss die Groß- und Kleinschreibung beachtet werden.
- Wenn Sie die gesamte Liste von Gruppenkonten erneut anzeigen möchten, geben Sie im Feld **Show users named** ein \* ein, oder löschen Sie dessen Inhalt, und klicken Sie dann auf **Update**.

## Schritt 4: Delegieren von Benutzerverwaltungsrechten (nur bei lokaler IVE-Authentifizierung)

### ☒ Delegieren von Benutzerverwaltungsrechten an Endbenutzer

Auf der Registerkarte **Authentication & Authorization > Authentication Servers > User Admins** können Sie Benutzerverwaltungsrechte an ausgewählte Endbenutzer delegieren, einschließlich der Rechte zum Hinzufügen von Benutzern zu einem Authentifizierungsserver, Löschen von Benutzern, Ändern der vollständigen Namen von Benutzern und Ändern der Kennwörter von Benutzern über das Menü **User Admin** auf der Startseite des sicheren Gateways.

**Hinweis:** Benutzeradministratoren können nur lokale IVE-Authentifizierungsserver verwalten. Beachten Sie außerdem, dass Benutzeradministratoren keine Gruppen oder Benutzer-zu-Gruppen-Zuordnungen verwalten können. Daher wird die Aktivierung des Benutzerverwaltungsfeatures nur dann empfohlen, wenn es die Regeln für die Benutzer-zu-Gruppen-Zuordnung auf dem Authentifizierungsserver Benutzern „ohne Übereinstimmung“ erlauben, sich beim IVE anzumelden (wie unter „Angaben von Informationen für die Gruppenzuordnung“ auf Seite 98 beschrieben), so dass der Benutzeradministrator neue Benutzer ohne Eingreifen des Administrators erfolgreich hinzufügen können. (Wenn die Benutzer-zu-Gruppen-Zuordnungen automatisch erfolgen, können Benutzeradministratoren die neuen Benutzer ohne Hilfe des Administrators manuell einer Autorisierungsgruppe zuordnen.)

### So delegieren Sie Benutzerverwaltungsrechte an einen Endbenutzer

1. Wählen Sie in der Administratorkonsole das Menü **Authentication & Authorization > Authentication Servers** aus.
2. Wählen Sie die lokale IVE-Authentifizierungsserverinstanz aus, die vom Benutzeradministrator verwaltet werden soll, und klicken Sie dann auf die Registerkarte **User Admins**.

---

**Hinweis:** Benutzeradministratoren können nur lokale IVE-Authentifizierungsserver verwalten.

---

3. Geben Sie den **Username** des Benutzers ein, der den ausgewählten Authentifizierungsserver verwalten soll. (Sie können zum Verwalten des lokalen IVE-Authentifizierungsserver einen beliebigen Benutzer



auswählen. Dieser muss dem zu verwaltenden Server nicht als lokaler Benutzer hinzugefügt werden.)

---

**Hinweis:** Achten Sie bei der Eingabe des Benutzernamens des Benutzeradministrators auf die exakte Zeichenfolge. Diese muss genau übereinstimmen.

---

4. Geben Sie den **Authentication Server** an, der das Benutzerkonto des im vorherigen Schritt ausgewählten Benutzeradministrators enthält.
5. Klicken Sie auf **Add**. Das IVE fügt den neuen Benutzeradministrator der Liste **User Admins** für den in Schritt 2 angegebenen Server hinzu und verwendet dabei folgendes Format: Benutzername@Servername.
6. Wenn der angegebene Benutzeradministrator über Benutzerkonten auf mehreren Authentifizierungsservern verfügt, wiederholen Sie optional für jedes dieser Konten die Schritte 3-5, so dass der Benutzer den Server unabhängig von dem Konto verwalten kann, über das er sich beim IVE angemeldet hat.
7. Um dem Benutzer die Verwaltungsrechte wieder zu entziehen, wählen Sie in der Liste **User Admins** den entsprechenden Namen aus, und klicken Sie auf **Remove**.

---

**Hinweis:** Informationen zum Verwalten von Benutzern über die Startseite des sicheren Gateways finden Sie in der Hilfe zum sicheren Gateway im Thema „Hinzufügen, Ändern und Löschen von Benutzern“.

---

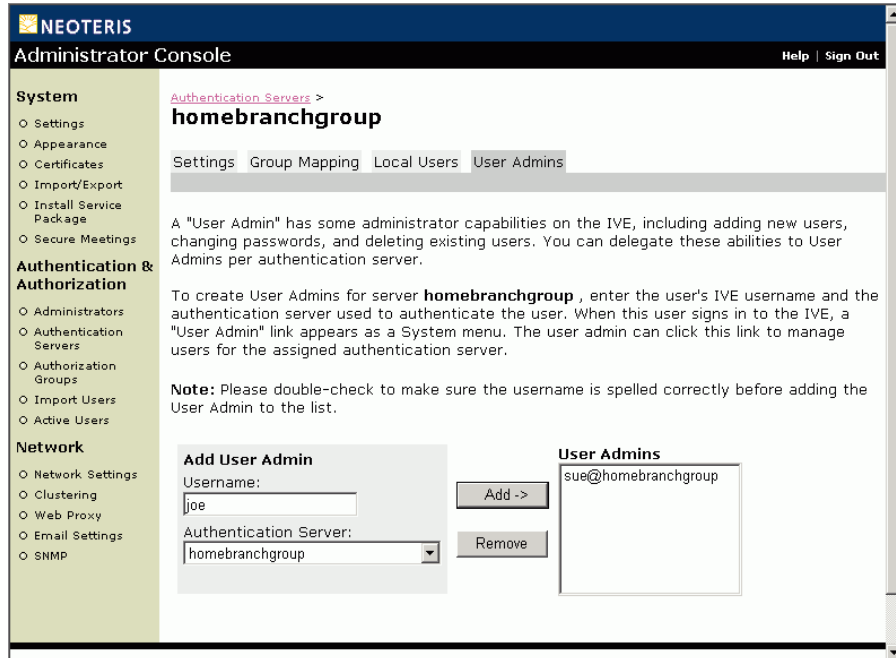


Abbildung 48: Authentication & Authorization > Authentication Servers > User Admins

---

## Ergänzende Informationen zur Konfiguration von Authentifizierungsservern

In diesem Abschnitt sind die Schritte zum Ausfüllen der Serverkonfigurationsseite für jeden der unterstützten Authentifizierungsserver beschrieben.

### ☒ Definieren einer Active Directory-Serverinstanz oder einer Windows NT-Domänenserverinstanz

Verwenden Sie diese Informationen zusammen mit den unter „Definieren einer Authentifizierungsserverinstanz“ auf Seite 92 beschriebenen Schritten.

### **So legen Sie einen Active Directory-Server oder einen Windows NT-Domänenserver fest**

1. Geben Sie einen Namen ein, um die Serverinstanz zu bezeichnen.
2. Geben Sie den Namen oder die IP-Adresse des primären Domänencontrollers oder von Active Directory an.
3. Geben Sie die IP-Adresse des Sicherungsdomänencontrollers oder von Active Directory an. (Optional.)
4. Geben Sie den Domänennamen für die Benutzer ein, denen Sie den Zugriff gewähren möchten.
5. Geben Sie unter **Authorization Group Settings** eine Option zum Zuordnen von Benutzern zu Gruppen ein. Eine Beschreibung dieser Optionen finden Sie auf Seite 93.
6. Klicken Sie auf **Save Changes**. Die Registerkarten **Group Mapping** und **Users** werden angezeigt.
7. Fahren Sie mit „Schritt 2: Angeben von Informationen für die Gruppenzuordnung“ auf Seite 98 fort.

**NEOTERIS**  
Administrator Console Help | Sign Out

**System**

- Settings
- Appearance
- Certificates
- Import/Export
- Install Service Package
- Secure Meetings

**Authentication & Authorization**

- Administrators
- Authentication Servers
- Authorization Groups
- Import Users
- Active Users

**Network**

- Network Settings
- Clustering
- Web Proxy
- Email Settings
- SNMP

[Authentication Servers >](#)  
**New NT Server**

Name:  Label to reference this server

Primary Domain Controller or Active Directory:  Name or IP address

Backup Domain Controller or Active Directory:  Name or IP address

Domain:  NT domain name

**Authorization Group Settings**

Specify how users will be mapped to authorization groups:

☐ Authorization group assigned based on querying a group lookup server

Server Properties:  Define...

☐ Authorization group assigned based on username

☒ All users are assigned to:

Authorization Group:

Save Changes Reset

**Abbildung 49: Authentication & Authorization > Authentication Servers > Active Directory or Windows NT Domain**

## ☑ Festlegen einer LDAP-Serverinstanz

Verwenden Sie diese Informationen zusammen mit den unter „Definieren einer Authentifizierungsserverinstanz“ auf Seite 92 beschriebenen Schritten.

### So legen Sie einen LDAP-Server fest

1. Geben Sie einen Namen ein, um die Serverinstanz zu bezeichnen.
2. Geben Sie den Namen oder die IP-Adresse des LDAP-Servers an, der vom Neoteris IVE zur Überprüfung von Benutzern verwendet wird.
3. Geben Sie den Port an, den der LDAP-Server überwacht. Dies ist bei Verwendung einer unverschlüsselten Verbindung normalerweise Port 389 und bei Verwendung von SSL Port 636.

4. Geben Sie Parameter für LDAP-Sicherungsserver an (optional). Das IVE verwendet die angegebenen Server für die Failover-Verarbeitung. Jede Authentifizierungsanforderung wird zunächst an den primären LDAP-Server weitergeleitet und dann an den oder die angegebenen Sicherungsserver, falls der primäre Server nicht erreichbar ist.

---

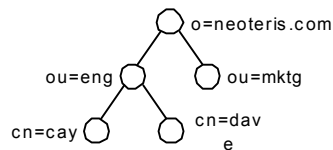
**Hinweis:** LDAP-Sicherungsserver müssen dieselbe Version wie der primäre LDAP-Server aufweisen. Beachten Sie auch, dass es beim Angeben von LDAP-Sicherungsservern ratsam ist, statt des Hostnamens die IP-Adresse anzugeben. Da der Hostname nicht in eine IP-Adresse aufgelöst werden muss, kann die Failover-Verarbeitung beschleunigt werden.

---

5. Geben Sie an, ob die Verbindung zwischen dem Neoteris IVE und dem LDAP-Verzeichnisdienst unverschlüsselt sein soll oder ob SSL (LDAPS) oder „LDAP over TLS“ verwendet werden soll.
6. Klicken Sie auf **Test Connection**, um die Verbindung zwischen dem IVE und den angegebenen LDAP-Servern zu prüfen. (Optional.)
7. Geben Sie den zu suchenden LDAP-Pfad an:
  - Wählen Sie **Static Distinguished Name (DN)**, um auf den DN eines Benutzers direkt zuzugreifen. Geben Sie den vollständigen DN-Pfad ein. Fügen Sie zur Verwendung des Benutzernamens, der auf der Anmeldeseite für die Suche eingegeben wird, im Pfad die Zeichenfolge <USER> (in Großbuchstaben) ein. Klicken Sie abschließend auf **Save Changes**.
  - Wählen Sie **Dynamic Distinguished Name (DN)**, um die Suche bei einer angegebenen Basis zu beginnen. Geben Sie im Feld **Base DN** den Pfad der Basis ein, bei der Sie die Suche beginnen möchten, und geben Sie optional einen **Filter\*** an, um die Suche einzugrenzen. Wenn das Neoteris IVE für das Durchsuchen der LDAP-Datenbank authentifiziert werden soll, aktivieren Sie **Require application (Neoteris IVE) authentication to search the LDAP database**, und geben Sie dann den Anwendungs-DN und das Kennwort an.

\*Fügen Sie zur Verwendung des Benutzernamens, der auf der Anmeldeseite für die Suche eingegeben wird, im Filter die Zeichenfolge <USER> (in Großbuchstaben) ein.

Beispiele:



- Wenn lediglich Techniker authentifiziert werden sollen, können Sie den statischen DN wie folgt festlegen:  
cn=<USER>,ou=eng,o=neoteris.com
  - Wenn alle Personen im Unternehmen authentifiziert werden sollen, können Sie den Basis-DN wie folgt festlegen:  
o=neoteris.com. Geben Sie optional\* in Großbuchstaben den Filter <USER> an.  
\*Es empfiehlt sich, einen Filter anzugeben, der keinen oder einen Benutzer-DN zurückgibt.
8. Geben Sie unter **Authorization Group Settings** eine Option zum Zuordnen von Benutzern zu Gruppen ein. Eine Beschreibung dieser Optionen finden Sie auf Seite 93.
  9. Klicken Sie auf **Save Changes**. Die Registerkarten **Group Mapping** und **Users** werden angezeigt.
  10. Fahren Sie mit „Schritt 2: Angeben von Informationen für die Gruppenzuordnung“ auf Seite 98 fort.

NEOTERIS

Administrator Console

Help | Sign Out

System

- Settings
- Appearance
- Certificates
- Import/Export
- Install Service Package
- Secure Meetings

Authentication & Authorization

- Administrators
- Authentication Servers
- Authorization Groups
- Import Users
- Active Users

Network

- Network Settings
- Clustering
- Web Proxy
- Email Settings
- SNMP

Authentication Servers >

New LDAP Server

Name:

Active Directory using LDAP

Label to reference this server

LDAP Server:

192.168.217.100

Name or IP address

LDAP Port:

389

Backup LDAP Server1:

Name or IP address

Backup LDAP Port1:

Backup LDAP Server2:

Name or IP address

Backup LDAP Port2:

Connection:

☒ Unencrypted

☐ LDAPS

☐ LDAP over TLS

Test Connection

☒ Static Distinguished Name (DN)

Directly access a user's DN. Enter the complete DN path, including <USER> to search for the username entered on the Sign-In page.

DN:

example: cn=<USER>,dc=sales,dc=com

☒ Dynamic Distinguished Name (DN)

Begin searching at a specified base. Enter the path to the base at which you want to begin the search. Specify a filter to fine-tune the search, including <USER> to search for the username entered on the Sign-In page.

Base DN:

dc=demo,dc=danastreet,dc=net

example: dc=sales,dc=com

Filter:

MAccountname=<USER>

example: cn=<USER>

☐ Require application (Neoteris IVE) authentication to search the LDAP database

Application DN:

Application password:

Authorization Group Settings

Specify how users will be mapped to authorization groups:

☒ Authorization group assigned based on attribute in authentication response

Group Attribute:

memberof

Name of the relevant attribute in the authentication response

☐ Authorization group assigned based on querying a group lookup server

Abbildung 50: Authentication & Authorization > Authentication Servers > LDAP Server

## ☑ Festlegen einer NIS-Serverinstanz

Verwenden Sie diese Informationen zusammen mit den unter „Definieren einer Authentifizierungsserverinstanz“ auf Seite 92 beschriebenen Schritten.

### So legen Sie einen NIS-Server fest

1. Geben Sie einen Namen ein, um die Serverinstanz zu bezeichnen.
2. Geben Sie den Namen oder die IP-Adresse des NIS-Servers an.
3. Geben Sie den Domännennamen für den NIS-Server an.
4. Geben Sie unter **Authorization Group Settings** eine Option zum Zuordnen von Benutzern zu Gruppen an. Eine Beschreibung dieser Optionen finden Sie auf Seite 93.
5. Klicken Sie auf **Save Changes**. Die Registerkarten **Group Mapping** und **Users** werden angezeigt.
6. Fahren Sie mit „Schritt 2: Angeben von Informationen für die Gruppenzuordnung“ auf Seite 98 fort.

---

**Hinweis:** Sie können nur eine NIS-Serverinstanz hinzufügen.

---



**NEOTERIS**  
Administrator Console Help | Sign Out

**System**

- Settings
- Appearance
- Certificates
- Import/Export
- Install Service Package
- Secure Meetings

**Authentication & Authorization**

- Administrators
- Authentication Servers
- Authorization Groups
- Import Users
- Active Users

**Network**

- Network Settings
- Clustering
- Web Proxy
- Email Settings
- SNMP

Authentication Servers >  
**New NIS Server**

Name:  Label to reference this server

NIS Server:  Name or IP address

NIS Domain:

**Authorization Group Settings**

Specify how users will be mapped to authorization groups:

☐ Authorization group assigned based on querying a group lookup server

Server Properties:  Define...

☐ Authorization group assigned based on username

☒ All users are assigned to:

Authorization Group:

Save Changes Reset

Abbildung 51: Authentication & Authorization > Authentication Servers > NIS

## ☑ Festlegen einer RADIUS-Serverinstanz

Verwenden Sie diese Informationen zusammen mit den unter „Definieren einer Authentifizierungsserverinstanz“ auf Seite 92 beschriebenen Schritten.

### So legen Sie einen RADIUS-Server fest

1. Geben Sie einen Namen ein, um die Serverinstanz zu bezeichnen.
2. Geben Sie den Namen oder die IP-Adresse des RADIUS-Servers ein.
3. Geben Sie die Portangabe für den RADIUS-Server ein. Normalerweise ist dies Port 1645.
4. Geben Sie eine Zeichenfolge für den gemeinsamen geheimen Schlüssel ein. Sie müssen diese Zeichenfolge beim Konfigurieren des RADIUS-Servers eingeben, damit die Neoteris IVE-Appliance als Client erkannt wird.

5. Klicken Sie abschließend auf **Save Changes**.
6. Konfigurieren Sie den RADIUS-Server durch folgenden Angaben so, dass der Neoteris IVE-Appliance-Server erkannt wird:
  - Hostname für die Neoteris IVE-Appliance.
  - Netzwerk-IP-Adresse der Neoteris IVE-Appliance.
  - Clienttyp der Neoteris IVE-Appliance (sofern vorhanden). Wenn diese Option verfügbar ist, wählen Sie „Single Transaction Server“ oder die entsprechende Option.
  - Verschlüsselungstyp für die Authentifizierung der Clientkommunikation. Die ausgewählte Option muss mit dem Clienttyp übereinstimmen.
  - Gemeinsamer geheimer Schlüssel, der in der Administratorkonsole auf der Seite **Network > Authentication > External Auth. Server > RADIUS** für den RADIUS-Server eingegeben wurde.
  - Zeitspanne, die das IVE auf eine Antwort vom RADIUS-Server bis zur Zeitüberschreitung für die Verbindung warten soll.
  - Anzahl der weiteren Versuche für das IVE, nach dem ersten fehlgeschlagenen Versuch eine Verbindung herzustellen.
  - Sekundären RADIUS-Server, der vom IVE verwendet wird, wenn der primäre, in dieser Instanz festgelegte, Server nicht erreichbar ist.

---

**Hinweis:** Für diesen sekundären RADIUS-Server müssen Sie eine Instanz festlegen.

---

7. Geben Sie unter **Authorization Group Settings** eine Option zum Zuordnen von Benutzern zu Gruppen ein. Eine Beschreibung dieser Optionen finden Sie auf Seite 93.
8. Klicken Sie auf **Save Changes**. Die Registerkarten **Group Mapping** und **Users** werden angezeigt.
9. Fahren Sie mit „Schritt 2: Angeben von Informationen für die Gruppenzuordnung“ auf Seite 98 fort.

NEOTERIS

Administrator Console

Help | Sign Out

System

- Settings
- Appearance
- Certificates
- Import/Export
- Install Service Package
- Secure Meetings

Authentication & Authorization

- Administrators
- Authentication Servers
- Authorization Groups
- Import Users
- Active Users

Network

- Network Settings
- Clustering
- Web Proxy
- Email Settings
- SNMP

Authentication Servers >

New Radius Server

Name:

Label to reference this server

Radius Server:

Name or IP address

Port:

1645

Shared Secret:

Timeout (in seconds):

30

Retries:

0

Secondary Radius Server:

Name or IP address

Secondary Radius Port:

Secondary Radius Secret:

Authorization Group Settings

Specify how users will be mapped to authorization groups:

Authorization group assigned based on attribute in authentication response

Attribute:

Name of the relevant attribute in the authentication response

Authorization group assigned based on querying a group lookup server

Server Properties:

(none)

Define...

Authorization group assigned based on username

All users are assigned to:

Authorization Group:

Users

Save Changes

Reset

Abbildung 52: Authentication & Authorization > Authentication Servers > Radius

## ☑ Festlegen einer ACE/Serverinstanz

Verwenden Sie diese Informationen zusammen mit den unter „Definieren einer Authentifizierungsserverinstanz“ auf Seite 92 beschriebenen Schritten.

### So legen Sie einen ACE/Server fest

1. Geben Sie einen Namen ein, um die Serverinstanz zu bezeichnen.

---

**Hinweis:** Wenn die Endbenutzer SecurID-Softwaretokens an ACE/Server übergeben (wie in „ACE/Server“ auf Seite 78 beschrieben), können Sie die Verwendung von Leerzeichen oder anderen nicht alphanumerischen Zeichen im Namen der Serverinstanz vermeiden. Um SecurID-Software-tokenwerte transparent an ACE/Server zu übergeben, müssen Benutzer unter Verwendung des folgenden URLs zur Seite **RSA SecurID Authentication** wechseln: <https://IVE/login/ServerInstanz> (wobei IVE die IP-Adresse oder den Hostnamen des IVE und ServerInstanz den oben festgelegten Namen darstellt). Wenn der Name der Serverinstanz Leerzeichen oder andere nicht alphanumerische Zeichen enthält, muss der Benutzer Escapezeichen (z. B. %20) in den URL einfügen.

---

2. Importieren Sie die RSA ACE/Agent-Konfigurationsdatei. Aktualisieren Sie diese Datei im Neoteris IVE unbedingt bei jeder Änderung an der Quelldatei. Ebenso müssen Sie, wenn Sie die Instanzdatei aus dem IVE löschen, zur Konfigurationsverwaltungsanwendung für ACE-Server wechseln, wie unter „Generieren einer ACE/Agent-Konfigurationsdatei“ auf Seite 117 beschrieben, und das Kontrollkästchen **Sent Node Secret** deaktivieren.
3. Informationen zum Erstellen der ACE-Serverkonfigurationsdatei finden Sie unter „Generieren einer ACE/Agent-Konfigurationsdatei“ auf Seite 117.
4. Geben Sie unter **Authorization Group Settings** eine Option zum Zuordnen von Benutzern zu Gruppen ein. Eine Beschreibung dieser Optionen finden Sie auf Seite 93.
5. Klicken Sie auf **Save Changes**. Die Registerkarten **Group Mapping** und **Users** werden angezeigt.
6. Fahren Sie mit „Schritt 2: Angeben von Informationen für die Gruppenzuordnung“ auf Seite 98 fort.

---

**Hinweis:** Sie können nur eine ACE/Serverinstanz hinzufügen.

---

## ☑ Generieren einer ACE/Agent-Konfigurationsdatei

Wenn Sie ACE/Server für die Authentifizierung verwenden, müssen Sie auf dem ACE-Server eine ACE/Agent-Konfigurationsdatei (`sdconf.rec`) für das IVE generieren.

### So generieren Sie eine ACE/Agent-Konfigurationsdatei

1. Starten Sie die Konfigurationsverwaltungsanwendung für ACE-Server, und klicken Sie auf **Agent Host**.
2. Klicken Sie auf **Add Agent Host**.
3. Geben Sie unter **Name** einen Namen für den IVE-Agenten ein.
4. Geben Sie unter **Network Address** die IP-Adresse des IVE ein.
5. Geben Sie eine auf dem ACE-Server konfigurierte **Site** an.
6. Wählen Sie als **Agent Type** den Typ **Communication Server** aus.
7. Wählen Sie als **Encryption Type** den Typ **DES** aus.
8. Vergewissern Sie sich, dass **Sent Node Secret** (beim Erstellen eines neuen Agenten) deaktiviert ist.

Wenn der ACE-Server eine vom IVE gesendete Anforderung erfolgreich authentifiziert, wählt der ACE-Server **Sent Node Secret** aus. Wenn der ACE-Server später einen neuen Knotenschlüssel an das IVE senden soll, gehen Sie bei der nächsten Authentifizierungsanforderung folgendermaßen vor:

1. Deaktivieren Sie das Kontrollkästchen **Sent Node Secret**, indem Sie auf dieses klicken.
  2. Melden Sie sich in der IVE-Administratorkonsole an, und wählen Sie im Hauptmenü den Eintrag **Authentication** aus.
  3. Wählen Sie im Untermenü die Option **External Servers** aus.
  4. Klicken Sie auf den Namen des ACE-Servers.
  5. Klicken Sie auf **Delete Node Verification File**. Durch diese Schritte wird sichergestellt, dass der IVE-Server und der ACE-Server synchronisiert sind. Entsprechend sollten Sie auf dem ACE-Server das Kontrollkästchen **Sent Node Secret** deaktivieren, wenn Sie die Überprüfungsdatei aus dem IVE löschen.
9. Klicken Sie auf **Assign Acting Servers**, und wählen Sie den ACE-Server aus.
  10. Klicken Sie auf **Generate Config File**.

Wenn Sie den ACE-Server zum IVE hinzufügen (wie in „Definieren einer Authentifizierungsserverinstanz“ auf Seite 92 beschrieben), wird diese Konfigurationsdatei importiert.

**NEOTERIS**  
Administrator Console Help | Sign Out

**System**

- Settings
- Appearance
- Certificates
- Import/Export
- Install Service Package
- Secure Meetings

**Authentication & Authorization**

- Administrators
- Authentication Servers
- Authorization Groups
- Import Users
- Active Users

**Network**

- Network Settings
- Clustering
- Web Proxy
- Email Settings
- SNMP

[Authentication Servers >](#)  
**New ACE Server**

Name:  Label to reference this server

ACE Port:

Configuration File:

Imported On:

**Import New Configuration File**

Config File:

**Delete Node Verification File**

<input type="checkbox"/>	Node	Creation Time
<input type="checkbox"/>	ive-1	-
<input type="checkbox"/>	ive-2	-

**Authorization Group Settings**

Specify how users will be mapped to authorization groups:

☐ Authorization group assigned based on querying a group lookup server

Server Properties:

☐ Authorization group assigned based on username

☒ All users are assigned to:

Authorization Group:

**Abbildung 53: Authentication & Authorization > Authentication Servers > ACE/Server**

## ☑ Festlegen einer Netegrity SiteMinder-Instanz

Verwenden Sie diese Informationen zusammen mit den unter „Definieren einer Authentifizierungsserverinstanz“ auf Seite 92 beschriebenen Schritten.

### So legen Sie einen Netegrity SiteMinder-Server fest

1. Geben Sie einen Namen ein, um die Serverinstanz zu bezeichnen.
2. Geben Sie im Feld **SiteMinder Server** den Namen oder die IP-Adresse des SiteMinder-Richtlinienservers ein. Sie können im Feld **SiteMinder Backup Server(s)** auch eine durch Kommas getrennte Liste von Richtliniensicherungsservern eingeben.

Wenn Sie einen oder mehrere Sicherungsserver eingeben, wählen Sie einen **Failover Mode** aus. Wählen Sie **Yes**, damit das IVE den Hauptrichtlinienserver verwendet, sofern dieser nicht ausfällt. Wählen Sie **No**, damit das IVE zwischen allen angegebenen Richtlinienservern einen Lastenausgleich vornimmt.

3. Geben Sie für **Secret** dem gemeinsamen geheimen Schlüssel und für **Agent Name** den Namen des Agenten an, die auf dem Richtlinienserver konfiguriert wurden.
4. Geben Sie im Feld **On logout, redirect to** einen URL an, an den Benutzer bei der Abmeldung vom IVE umgeleitet werden (wenn Benutzern die beim Abmelden standardmäßig angezeigte IVE-Anmeldeseite nicht angezeigt werden soll).
5. Geben Sie im Feld **Policy Server Poll Interval** das Intervall ein, in dem der SiteMinder-Richtlinienserver den Verschlüsselungsschlüssel für die Kommunikation mit den Web-Agenten ändert. Das IVE sucht im angegebenen Intervall nach einem neuen Schlüssel.
6. Zur Leistungssteigerung können Sie ggf. die Einstellungen für die Verbindung und für Leerlaufzeitlimits abstimmen. Beachten Sie jedoch die empfohlenen Standardeinstellungen:
  - **Maximum Number of Connections to Policy Server:** 20
  - **Maximum Number of Requests Per Policy Server Connection:** 1000
  - **Policy Server Connection Idle Timeout:** none
7. Ändern Sie ggf. die Ports, die das IVE für Verbindungen mit dem SiteMinder-Richtlinienserver verwendet. Im Folgenden finden Sie die Standardeinstellungen:
  - **Policy Server Accounting Port:** 44441
  - **Policy Server Authentication Port:** 44442
  - **Policy Server Authorization Port:** 44443

8. Unter **Protected resource and action**:

- 1 Wir empfehlen, die Standardeinstellung `/siteminder` im Feld **Protected Resource** zu akzeptieren. Wenn sich ein Benutzer anmeldet, wird er mit dieser vom Administrator angegebenen geschützten Ressource über den SiteMinder-Richtlinienserver authentifiziert.
- 2 Geben Sie die Ressourcenaktion ein, die der für den SiteMinder-Richtlinienserver festgelegten Aktion entspricht (GET, POST, PUT usw.).

Weitere Informationen finden Sie unter „Konfigurieren des IVE als Web-Agent auf einem SiteMinder-Richtlinienserver“ auf Seite 123.

9. Unter **SMSESSION cookie settings**:

- 1 Geben Sie im Feld **Cookie Domain** die Internetdomäne ein, in der das Cookie gültig ist und an die der Browser des Benutzers Cookieinhalte sendet. Diese Cookiedomäne muss mit der IVE-Domäne übereinstimmen.
- 2 Geben Sie im Feld **Cookie Provider Domain** die Internetdomäne (oder eine durch Kommas getrennte Liste von Domänen) ein, in der das Cookie gültig ist und an die das IVE Cookieinhalte sendet. Wenn Sie einen Cookieanbieter konfiguriert haben, geben Sie die Domäne des Cookieanbieters ein. Andernfalls geben Sie die Domäne der Web-Agenten ein, für die eine Einzelanmeldung gewünscht wird.
- 3 Wenn andere Web-Agenten zum Akzeptieren sicherer Cookies konfiguriert wurden, wählen Sie für **Send cookie securely?** die Option **Yes** aus. Das Cookie wird dann nur über HTTPS übermittelt. Um ein Cookie über nicht sicheres HTTP zu senden, wählen Sie **No**.

10. Unter **SiteMinder Authentication**:

- 1 Wenn Benutzer, die über ein gültiges SMSESSION-Cookie verfügen, automatisch angemeldet werden sollen, aktivieren Sie das Kontrollkästchen **Automatic Sign-In**, und wählen Sie dann eine IVE-Gruppe aus. Verwenden Sie diese Option, um Benutzern die Einzelanmeldung zu ermöglichen. Diese Option ermöglicht es Benutzern, sich bei einem Standardweb-Agenten anzumelden, der ein SMSESSION-Cookie generiert. Wenn ein Benutzer auf eine Verknüpfung mit dem IVE (Hostname) klickt, wird dieses Cookie an das IVE übergeben, und die Benutzer werden nicht aufgefordert, ihre Anmeldeinformationen erneut zu senden. Alle Benutzer, die sich auf diese Art im IVE anmelden, werden der von Ihnen angegebenen Benutzergruppe zugeordnet. Außerdem werden alle von Ihnen für diese Gruppe angegebenen Zugriffssteuerungen angewendet.



---

**Hinweis:** Die automatische Anmeldeoption stellt für die Benutzer eine alternative Art dar, sich im IVE anzumelden. Sie können auch unter **Authorization Group Settings** eine Option zum Zuordnen von Benutzern zu Gruppen konfigurieren. Wenn Benutzer sich über die IVE-Standardanmeldeseite direkt im IVE anmelden, werden sie Autorisierungsgruppen auf der Grundlage von Autorisierungsgruppeneinstellungen zugeordnet.

---

- 2 Wählen Sie eine Methode für die Cookieauthentifizierung aus:
- **Authenticate using custom agent**—Wählen Sie diese Option aus, wenn Sie die Authentifizierung über das IVE vornehmen möchten.
  - **Authenticate using HTML form post**—Wählen Sie diese Option aus, wenn die Authentifizierung mit Hilfe eines anderen Web-Agenten vorgenommen werden soll. Geben Sie die Einstellungen für die Formularbereitstellung an:

Einstellung	Beschreibung
<b>Ziel</b>	URL auf dem externen, Netegrity-fähigen Webserver.
<b>Protokoll</b>	Protokoll für die Kommunikation zwischen IVE und dem angegebenen Web-Agenten. Verwenden Sie HTTP für die nicht sichere Kommunikation oder HTTPS für die sichere Kommunikation.
<b>Web-Agent</b>	Name des Web-Agenten, von dem das IVE SMSESSION-Cookies abrufen soll. Eine IP-Adresse kann in diesem Feld nicht eingegeben werden. Wenn die IP-Adresse als Web-Agent angegeben wird, können manche Browser keine Cookies akzeptieren.
<b>Port</b>	Port 80 für HTTP oder Port 443 für HTTPS.
<b>Pfad</b>	Pfad der Anmeldeseite des Web-Agenten.
<b>Parameter</b>	Post-Parameter, die bei der Anmeldung eines Benutzers gesendet werden. Standardmäßig verwendet das IVE die Variablen <code>_USER_</code> , <code>_PASS_</code> und <code>_TARGET_</code> . Diese Variablen werden durch den vom Benutzer auf der Anmeldeseite des Web-Agenten eingegebenen Benutzernamen und das Kennwort sowie durch den im Feld <b>Target</b> angegebenen Wert ersetzt.

11. Geben Sie im Feld **If authentication fails, redirect to** einen alternativen URL ein, an den Benutzer (statt an die IVE-Anmeldeseite) umgeleitet werden, wenn der Benutzer vom IVE nicht authentifiziert werden kann. Dieser URL wird nur dann verwendet, wenn vom SiteMinder-Richtlinienserver keine Antwort zum Umleiten empfangen wurde.
12. Aktivieren Sie unter **SiteMinder Authorization** die Option **Authorize each request against SiteMinder**, um Webressourcenanforderungen von Benutzern mit den Regeln des SiteMinder-Richtlinienservers zu autorisieren. Wenn Sie diese Option auswählen, speichert das IVE Berechtigungen für Benutzeranforderungen für zehn Minuten im Cache. Wenn ein Benutzer während dieser zehn Minuten mehrmals auf dieselbe Ressource zugreift, muss die Anforderung nicht erneut gesendet werden. Um diesen Cache manuell zu leeren, klicken Sie auf **Flush Cache**.  
Wenn Sie diese Option auswählen, müssen Sie in SiteMinder die entsprechenden Regeln erstellen, die mit dem Servernamen gefolgt von einem Schrägstrich beginnen, z. B.: „www.yahoo.com/“, „www.yahoo.com/\*“ und „www.yahoo.com/r/f1“.

Nächster Schritt:

- 1 Geben Sie einen URL ein, an den das IVE Benutzer umleitet, deren Authentifizierung fehlschlägt. Diese Seite wird anstelle einer IVE-Fehlermeldung angezeigt.

---

**Hinweis:** Das IVE verwendet diesen Umleitungs-URL nur dann, wenn vom SiteMinder-Richtlinienserver keine Antwort zum Umleiten empfangen wird.

---

- 2 Geben Sie im Feld **Resource for insufficient protection level** eine Ressource des Web-Agenten ein, an die Benutzer vom IVE umgeleitet werden, wenn sie nicht über die erforderlichen Berechtigungen verfügen. Diese Ressource ist statisch. Schreiben Sie daher auf der Seite, zu die der Benutzer umgeleitet wird, eine allgemeine Meldung.

Sie können Benutzer zum Beispiel zu einer Anmeldeseite umleiten. Beachten Sie, dass Sie nicht den gesamten URL der Ressource eingeben müssen (z. B. „http://www.StdWebAgent.com/index.html“). Sie müssen nur die Ressource eingeben (hier „index.html“).

---

**Hinweis:** Wenn Sie Version 5.5 oder eine höhere Version des Web-Agenten mit V5QMR3 verwenden, können Sie Benutzer mit unzureichenden Berechtigungen zu deren ursprünglicher Ressource zurückleiten, indem Sie in der Administratorkonsole das Feld **Resource for insufficient protection level** leer lassen und den Kompatibilitätsmodus für Formularanmeldeinformationen-Collector des Web-Agenten für das Netegrity Agent Conf-Objekt deaktivieren (FCCCompatMode=no).

---

- 3 Geben Sie Dateierweiterungen ein, die den Dateitypen entsprechen, für die keine Autorisierung erforderlich ist.

13. Geben Sie unter **Authorization Group Settings** eine Option zum Zuordnen von Benutzern zu Gruppen ein. Eine Beschreibung dieser Optionen finden Sie auf Seite 93.

---

**Hinweis:** Die unter **Authorization Group Settings** festgelegte Option zum Zuordnen von Benutzern zu Gruppen wird bei der Anmeldung von Benutzern auf der IVE-Standardanmeldeseite angewendet. Wenn für die Benutzer die Einzelanmeldung bereitgestellt werden soll, konfigurieren Sie die Option **Automatic Sign-In** (Schritt 10), und verweisen Sie die Benutzer zu dem Web-Agenten, der das vom IVE verwendete SMSESSION-Cookie erzeugt.

---

14. Klicken Sie auf **Save Changes**. Die Registerkarten **Group Mapping** und **Users** werden angezeigt.
15. Fahren Sie mit „Schritt 2: Angeben von Informationen für die Gruppenzuordnung“ auf Seite 98 fort.

## ☒ Konfigurieren des IVE als Web-Agent auf einem SiteMinder-Richtlinienserver

Sie können einen SiteMinder-Server erst als IVE-Authentifizierungsserver hinzufügen, wenn Sie das IVE auf dem SiteMinder-Richtlinienserver als Agenten konfiguriert haben. Das folgende Verfahren enthält die grundlegenden Schritte zur Konfiguration eines SiteMinder-Richtlinienservers. Weitere Informationen finden Sie in der Dokumentation zu Ihrem SiteMinder-Server.

### **So konfigurieren Sie das IVE als Web-Agent auf einem SiteMinder-Richtlinienserver**

1. Melden Sie sich auf der Benutzeroberfläche des Richtlinienservers an.
2. Erstellen Sie einen Agenten für das IVE. Wenn Sie SiteMinder, Version 5, verwenden, erstellen Sie ein Hostkonfigurationsobjekt, oder duplizieren Sie ein vorhandenes Hostkonfigurationsobjekt, und ändern Sie die Parameterwerte.
3. Konfigurieren Sie eine neue Richtliniendomäne, oder verwenden Sie eine vorhandene Richtliniendomäne.

4. Erstellen Sie innerhalb der Richtliniendomäne einen Bereich. Legen Sie den Ressourcenfilter auf „/“ fest, und legen Sie dann eine GET-Regel fest, um alle Ressourcen mit „\*“ zu schützen. Stellen Sie sicher, dass Sie die entsprechenden Einstellungen für „Protected Resource“ und „Resource Action“ verwenden, wenn Sie später die SiteMinder-Authentifizierungsservereinstellungen in der IVE-Administratorkonsole konfigurieren.

---

**Hinweis:** Wenn der Bereichsressourcenfilter auf „/“ festgelegt wird, entsprechen die durch den benutzerdefinierten IVE-Agenten an den Richtlinienserver übergebenen Ressourcen der Regel. Wenn Sie den Ressourcenfilter weiter einschränken möchten, muss der in der IVE-Administratorkonsole angegebene Ressourcenfilter der Regel entsprechen. Standardmäßig wird der Ressourcenfilter in den IVE-SiteMinder-Serveroptionen auf „/siteminder“ festgelegt.

---

5. Erstellen Sie innerhalb der Richtliniendomäne eine Richtlinie, die die Regeln vorhandenen Benutzerverzeichnissen zuordnet.

NEOTERIS

Administrator Console

Help | Sign Out

System

- Settings
- Appearance
- Certificates
- Import/Export
- Install Service Package
- Secure Meetings

Authentication & Authorization

- Administrators
- Authentication Servers
- Authorization Groups
- Import Users
- Active Users

Network

- Network Settings
- Clustering
- Web Proxy
- Email Settings
- SNMP

Authentication Servers >

New Siteminder Server

Name:

Label to reference this server

SiteMinder Server:

Name or IP address

SiteMinder Backup Server(s):

Comma-delimited list of names or IP addresses

Failover Mode?

Yes

No

Secret:

Agent Name:

Name configured on Policy Server

On logout, redirect to:

Policy Server Poll Interval:

none

Seconds, use "none" to turn off polling

Maximum Number of Connections to Policy Server:

20

Allowed values range between 1 and 2048

Maximum Number of Requests Per Policy Server Connection:

1000

Allowed values range between 1 and 10000

Policy Server Connection Idle Timeout:

none

Minutes, use "none" to indicate no limit. Allowed values range between 1 and 35791394

Policy Server Accounting Port:

44441

Policy Server Authentication Port:

44442

Policy Server Authorization Port:

44443

Protected resource and action

These fields are used by the system during custom agent authentication and cookie verification

Protected Resource:

/siteminder

example: /siteminder

Resource Action:

GET

example: GET

SMSESSION cookie settings

These fields are used by the system during cookie verification

Cookie Domain:

Used when setting cookie in the end-user's browser. example: live.company.com

Cookie Provider Domain:

Used when sending cookie to the SiteMinder cookie provider. example: .company.com

Send cookie securely?

Yes

No

If yes, cookies are sent using HTTPS. Note that cookies sent to end-user's browser are always sent securely.

SiteMinder Authentication

These settings control authentication with SiteMinder.

Automatic Sign In

Check if you want users with a valid SMSESSION cookie to be automatically signed in.

They will be assigned to this group: 

None

Authenticate using custom agent

Authenticate using HTML form post

Target:

Resource on the external Netegrity enabled webserver. example: http://wa.webagent.com/Default.htm

Protocol:

HTTP

HTTPS

Webagent:

Fully qualified name of the external Netegrity enabled webserver. example: wa.webagent.com

Port:

80

Path:

/siteminderagent/forms/login.fcc

Parameters:

user=\_\_USER\_\_&password=\_\_PASS\_\_&target=\_\_

Abbildung 54: Authentication & Authorization > Authentication Servers > SiteMinder

## Menü „Authentication & Authorization > Authorization Groups“

Verwenden Sie die Registerkarten **Authentication & Authorization > Authorization Groups**, um Autorisierungsgruppen <sup>1</sup> zu erstellen und zu verwalten. Dazu gehören folgende Aufgaben:

- Überprüfen einer Zusammenfassung der Einstellungen für Autorisierungsgruppen (127)
- Angeben von Zeitbegrenzungen und Roamingfunktionen für Autorisierungsgruppen (133)
- Angeben von Benutzeranmeldeinformationen und der Beständigkeit von IVE-Sitzungscookies (135)
- Überprüfen der Zuordnungen von Servern zu Gruppen (137)
- Einschränken der möglichen IP-Adressen für die Benutzeranmeldung (138)
- Einschränken der möglichen Browser für die Benutzeranmeldung (139)
- Festlegen, dass Clientcomputer über ein gültiges Zertifikat verfügen müssen (142)
- Festlegen von allgemeinen Einstellungen für Webbrowsing (148)
- Zugriffssteuerung für Webressourcen (158)
- Erstellen von Lesezeichen für Webressourcen (161)
- Angeben der Server, mit denen Java-Applets eine Verbindung herstellen können (163)
- Steuern des Netzwerkzugriffs unter Windows und UNIX/NFS (164)
- Zugriffssteuerung für Windows-Ressourcen (167)
- Erstellen von Lesezeichen für Windows-Ressourcen (170)
- Zugriffssteuerung für UNIX/NFS-Ressourcen (172)
- Erstellen von Lesezeichen für UNIX-Ressourcen (174)
- Aktivieren der Aktualisierungsoption für den Secure Email Client (176)
- Angeben von allgemeinen Client-/Server-Anwendungseinstellungen (178)

---

1. Für Autorisierungsgruppen ist in einigen IVE-Produkten eine Lizenz erforderlich.

- Konfigurieren der externen DNS-Server und Benutzercomputer (falls erforderlich) (201)
- Konfigurieren eines PCs, der die Verbindung mit dem IVE über einen Proxywebserver herstellt (202)
- Testen von J-SAM im Unternehmen (203)
- Erstellen von Lesezeichen für sichere Terminalsitzungen (185)
- Festlegen von Anwendungen und Hosts, die mit W-SAM gesichert werden sollen. (189)
- Festlegen von Clientanwendungen, für die J-SAM eine Portweiterleitung durchführt (197)
- Angeben zulässiger MS Exchange-Server (207)
- Festlegen zulässiger Lotus Notes-Server (211)
- Konfigurieren des Lotus Notes-Clients (213)
- Ändern von Citrix NFuse-StandardEinstellungen (215)

## General > Unterregisterkarte „Overview“

### ☒ Überprüfen einer Zusammenfassung der Einstellungen für Autorisierungsgruppen

Verwenden Sie diese Registerkarte, um eine Zusammenfassung der Einstellungen für Autorisierungsgruppen zu überprüfen.

#### **So überprüfen Sie eine Zusammenfassung der Gruppeneinstellungen**

1. Wählen Sie in der Administratorkonsole das Menü **Authentication & Authorization > Authorization Groups** und anschließend eine Gruppe aus.
2. Wählen Sie aus den Gruppenregisterkarten **General > Overview** aus.

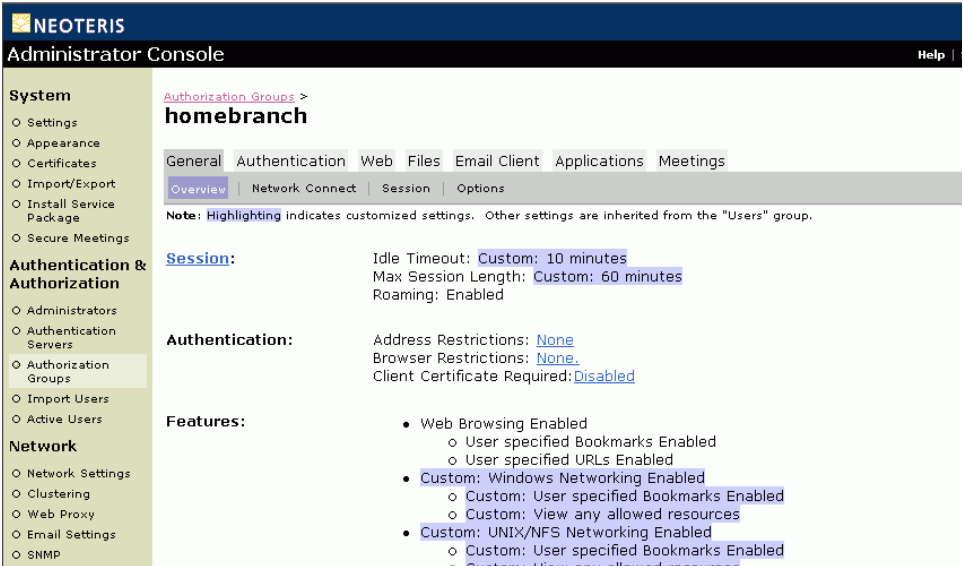


Abbildung 55: Authentication & Authorization > GroupName > General > Overview



## General > Unterregisterkarte Network Connect

Über die Aktualisierungsoption „Network Connect“ verfügen Sie auf Netzwerkebene über einen sicheren, SSL-basierten Remotezugriff auf alle Unternehmensanwendungsressourcen über das IVE. W-SAM (Seite 187) bietet im Vergleich zu Network Connect eine höhere Sicherheit, jeddoch können Hauptbenutzer, die einen Netzwerkzugriff benötigen, auch die Option Network Connect verwenden.

---

**Wichtig:** Die Benutzer müssen auf ihrem Windows-PC über Administratorberechtigungen verfügen, so dass die Network Connect-Softwarekomponenten vom IVE auf dem PC installiert werden können.

---

## Übersicht über Network Connect

Die Option Network Connect bietet Möglichkeiten zur Verwendung eines VPN ohne Client und dient als zusätzlicher Mechanismus für den Remotezugriff auf Unternehmensressourcen über das IVE. Dieses Feature unterstützt alle Modi für den Internetzugang (einschließlich DFÜ-Verbindungen, Breitband und LAN-Szenarien) vom Clientcomputer aus und funktioniert bei Vorhandensein clientseitiger Proxys und Firewalls, die den SSL-Datenverkehr über Port 443 zulassen.

Wenn ein Benutzer Network Connect startet, wird der gesamte Datenverkehr zum und vom Client über den sicheren Network Connect-Tunnel übertragen. Die einzige Ausnahmeroute besteht für Datenverkehr, der von anderen IVE-fähigen Features initiiert wird, z. B. Durchsuchen von Web und Dateien sowie Telnet/SSH. Wenn Sie für bestimmte Benutzer keine anderen IVE-Features aktivieren möchten, erstellen Sie eine Autorisierungsgruppe, für die nur die Option Network Connect aktiviert ist. Dieser Gruppe zugeordneten Benutzer wird auf der IVE-Startseite nur die Verknüpfung für Network Connect angezeigt.

Da der gesamte PC-Datenverkehr über den Network Connect-Tunnel zu den internen Unternehmensressourcen übertragen wird, müssen Sie sicherstellen, dass andere Hosts in demselben lokalen Netzwerk wie der PC keine Verbindung mit dem PC herstellen können, auf dem Network Connect ausgeführt wird. Wir empfehlen, dass Clients vor dem Starten einer Remotezugriffssitzung auf Netzwerkebene Lösungen für die Endpunktsicherheit ausführen müssen, z. B. eine persönliche Firewall. Informationen zum Überprüfen, ob Clients Software für die Endpunktsicherheit verwenden, finden Sie unter „Durchführen einer clientseitigen Überprüfung der Software für die Endpunktsicherheit“ auf Seite 145.

Die Network Connect-Anwendung wird wie folgt ausgeführt:

1. Ein Benutzer meldet sich im IVE an und klickt auf der IVE-Startseite auf die Verknüpfung für **Network Connect**. Daraufhin wird der Benutzer in einer Warnung aufgefordert, sicherzustellen, dass die Arbeitsstation vertrauenswürdig und sicher ist.
2. Anschließend wird vom IVE ein Active X-Steuerelement auf den Clientcomputer heruntergeladen, das die folgenden Aktionen ausführt:
  - 1 Das IVE ermittelt, ob Network Connect installiert ist. Wenn dies nicht der Fall ist, installiert das IVE die erforderliche Software in einem einmaligen Setup.
  - 2 Der Dienst Network Connect sendet eine Anforderung an das IVE, um die Verbindung mit einer IP-Adresse aus dem zuvor bereitgestellten IP-Pool zu initialisieren.
  - 3 Das System Tray-Symbol für Network Connect wird auf der Taskleiste angezeigt.
3. Die serverseitige Network Connect-Software weist dem Client für die Sitzung eine eindeutige IP-Adresse aus dem konfigurierten Pool zu.
4. Der Network Connect-Client verwendet die vom IVE zugewiesene IP-Adresse für die Kommunikation mit Unternehmensressourcen. Die gesamte Network Connect-Kommunikation wird über das IVE übertragen.

## ☒ Aktivieren und Konfigurieren Network Connect

Auf der Unterregisterkarte **General > Network Connect** können Sie die Network Connect-Aktualisierungsoption aktivieren und konfigurieren. Zum Konfigurieren der Network Connect-Option müssen Sie einen IP-Pool angeben, aus dem das IVE Clients IP-Adressen zuweisen kann. Bei einem eigenständigen IVE müssen Sie für den Router eine statische Route konfigurieren, die auf die interne IP-Adresse des IVE als Gateway für die Route zeigt. Wenn Sie ein Clusterpaar oder einen Multi-Unit-Cluster ausführen, erstellen Sie für den Router eine zusätzliche IP-Adresse für jeden Clusterknoten. Dabei muss sich jede IP-Adresse in demselben Subnetz wie der entsprechende IP-Pool befinden.

## So konfigurieren Sie die Network Connect-Option

1. Wählen Sie in der Administratorkonsole das Menü **Authentication & Authorization > Authorization Groups** und anschließend eine Gruppe aus.
2. Wählen Sie aus den Gruppenregisterkarten **General > Network Connect** aus.  
Benutzerdefinierte Autorisierungsgruppen erben standardmäßig die Einstellungen der Benutzergruppe. Klicken Sie zum Festlegen benutzerdefinierter Einstellungen auf **Use custom settings** und anschließend auf **Update**.
3. Wählen Sie **Enable Network Connect Option**, und klicken Sie auf **Save Changes**.
4. Geben Sie unter **Client Address Pool** IP-Adressen oder einen Bereich von IP-Adressen an, die vom IVE Clients zugewiesen werden sollen, die den Dienst Network Connect ausführen.
5. Geben Sie unter **Access Control** die IP-Adresse, die Netzmaske und den Port bzw. Portbereich für eine Netzwerkressource an, die für Network Connect verfügbar sein soll. Sie können auch das Protokoll angeben, über das der Client mit der Netzwerkressource kommuniziert, u. a. TCP, UDP oder ICMP. Wenn Sie **All** auswählen, werden Anfragen in einem der drei Protokolle vom IVE weitergeleitet.

### Hinweis:

- Das ICMP-Protokoll kann für den Zugriff auf Netzwerkressourcen nicht verwendet werden, für die Sie einen Port oder Portbereich angeben.
- In der Standardeinstellung kann auf alle Netzwerkressourcen zugegriffen werden. Wenn Sie der Zugriffssteuerungsliste eine Ressource hinzufügen, sind jedoch nur diese Ressource und nachfolgend hinzugefügte Ressourcen für Benutzer verfügbar.

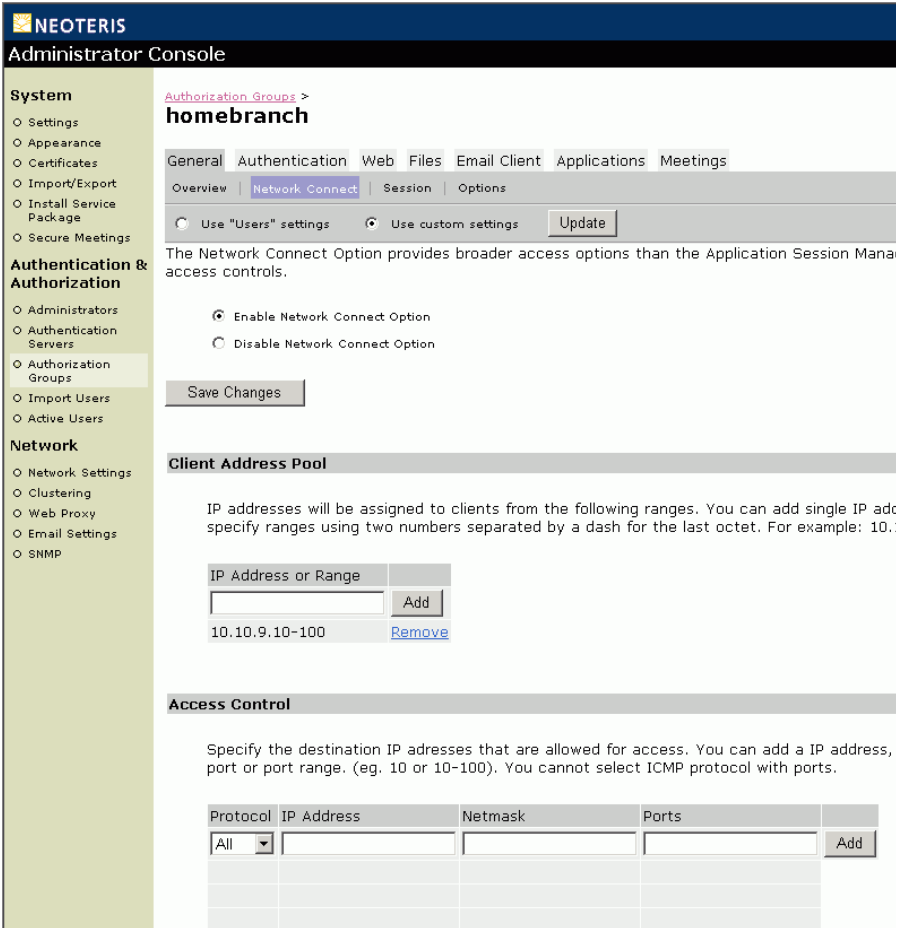


Abbildung 56: Authentication & Authorization > Authorization Groups > GroupName > General > Network Connect

## General > Unterregisterkarte „Session“

### ☒ Angeben von Zeitbegrenzungen und Roamingfunktionen für Autorisierungsgruppen

Auf dieser Registerkarte können Sie folgende Angaben vornehmen:

- **Time limits for user sessions**

Die Standardzeitbegrenzung für eine Benutzersitzung beträgt sechzig Minuten. Nach dieser Zeitspanne beendet das IVE die Benutzersitzung und protokolliert das Ereignis im Systemprotokoll. Die Leerlaufzeitbegrenzung für Sitzungen beträgt in der Standardeinstellung zehn Minuten, d. h., eine Benutzersitzung, die zehn Minuten lang inaktiv ist, wird vom IVE beendet, und das Ereignis wird im Systemprotokoll protokolliert.

- **Roamingfunktionen für Benutzersitzungen**

Eine Roamingbenutzersitzung funktioniert über Quell-IP-Adressen, wodurch sich mobile Benutzer (Benutzer von Laptops) mit dynamischen IP-Adressen von einem Standort aus im IVE anmelden können und Ihre Arbeit von einem anderen Standort fortsetzen können. Einige Browser weisen jedoch eventuell Schwachstellen auf, über die durch böswilligen Code Benutzercookies gestohlen werden können. Ein böswilliger Benutzer kann dann ein gestohlenes IVE-Sitzungscookie verwenden, um sich im IVE anzumelden.

### So geben Sie Zeitbegrenzungen und Roamingfunktionen für Autorisierungsgruppen an

1. Wählen Sie in der Administratorkonsole das Menü **Authentication & Authorization > Authorization Groups** und anschließend eine Gruppe aus.
2. Wählen Sie auf den Gruppenregisterkarten die Option **Session** aus.
3. Unter **Session timeout**:
  - 1 Wählen Sie **Use custom settings** aus, und klicken Sie dann auf **Save Changes**, wenn Sie für eine Autorisierungsgruppe neue Sitzungszeitüberschreitungen angeben möchten.
  - 2 Geben Sie die Anzahl der Minuten an, die sich eine nicht administrative Benutzersitzung im Leerlauf befinden kann, bevor sie beendet wird. Die Mindestzeit beträgt drei Minuten.
  - 3 Geben Sie die Anzahl der Minuten an, die eine aktive nicht administrative Benutzersitzung geöffnet bleiben kann, bevor sie beendet wird. Die Mindestzeit beträgt drei Minuten.
4. Wählen Sie unter **Enable roaming session** eine der folgenden Optionen aus:

- **User „Users“ settings**  
Wendet die Einstellungen der Benutzergruppe an.
- **Enabled (maximize mobility)**  
Benutzer können sich von einer IP-Adresse aus anmelden und ihre Sitzung von einer anderen IP-Adresse aus fortsetzen.
- **Limited to subnet range (minimum mobility, increased security)**  
Benutzer können sich von einer IP-Adresse aus anmelden und ihre Sitzungen mit einer anderen IP-Adresse fortsetzen, sofern sich die neue IP-Adresse in demselben Subnetz befindet. Wenn Sie diese Option auswählen, geben Sie eine Netzmaske an, die das Subnetz definiert.
- **Disabled (maximize security)**  
Benutzer, die sich von einer IP-Adresse aus anmelden, können eine aktive IVE-Sitzung nicht von einer anderen IP-Adresse aus fortsetzen. Benutzersitzungen sind an die ursprüngliche Quell-IP-Adresse gebunden.

5. Klicken Sie auf **Save Changes**.

The screenshot shows the NEOTERIS Administrator Console interface. The left sidebar contains a navigation menu with categories: System, Authentication & Authorization, and Network. The 'Authentication & Authorization' section is expanded, showing 'Authorization Groups' as the selected item. The main content area displays the configuration for the 'homebranch' group, with tabs for General, Authentication, Web, Files, Email Client, Applications, and Meetings. The 'Session timeout' section is active, showing options for 'Use "Users" settings' and 'Use custom settings'. The 'Use custom settings' option is selected, with 'Idle Timeout' set to 10 minutes and 'Max. Session Length' set to 60 minutes. Below this, the 'Enable roaming session' section is shown, with the 'Use "Users" settings (Enabled)' option selected. The 'Enabled (maximize mobility)' option is also visible, with a description: 'Sessions work across source IP addresses.' The 'Limited to subnet range (minimum mobility, increased security)' option is also visible, with a description: 'Sessions work within this subnet' and a 'Netmask' input field. The 'Disabled (maximize security)' option is also visible, with a description: 'Sessions are tied to the initial source IP address.' A 'Save Changes' button is located at the bottom of the configuration area.

Abbildung 57: Authentication & Authorization > GroupName > General > Session

## General > Unterregisterkarte „Options“

### ☒ **Angeben von Benutzeranmeldeinformationen und der Beständigkeit von IVE-Sitzungscookies**

Auf dieser Registerkarte können Sie die Beständigkeit von Benutzeranmeldeinformationen über mehrere Sitzungen sowie die Beständigkeit einer IVE-Sitzung über Browserinstanzen angeben.

#### **So geben Sie Benutzeranmeldeinformationen und die Beständigkeit von IVE-Sitzungscookies an**

1. Wählen Sie in der Administratorkonsole das Menü **Authentication & Authorization > Authorization Groups** und anschließend eine Gruppe aus.
2. Wählen Sie aus den Gruppenregisterkarten **General > Options** aus.
3. Aktivieren oder deaktivieren Sie die jeweiligen Optionen, und klicken Sie anschließend auf **Save changes**. Folgende Optionen stehen zur Verfügung:

- **Enable Persistent Password Caching**

Der Neoteris IVE-Server unterstützt die NTLM- und HTTP-Standardauthentifizierung sowie Server, die sowohl für NTLM-Anmeldungen als auch für anonyme Anmeldungen eingerichtet sind. Das IVE speichert von Benutzern eingegebene Kennwörter für die NTLM- und HTTP-Standardauthentifizierung im Cache, so dass die Benutzer nicht wiederholt aufgefordert werden, die Anmeldeinformationen einzugeben, die bereits bei der Anmeldung beim IVE-Server oder einer anderen Ressource in der NT-Domäne verwendet wurden. Standardmäßig leert der IVE-Server zwischengespeicherte Kennwörter aus dem Cache, wenn sich ein Benutzer abmeldet. Verwenden Sie diese Option, damit zwischengespeicherte Kennwörter über mehrere Sitzungen für eine Gruppe weiterbestehen können. Ein Benutzer kann zwischengespeicherte Kennwörter über die Seite **Advanced Preferences** löschen.

- **Enable Persistent Session Cookies**

Standardmäßig wird das IVE-Sitzungscookie aus dem Speicher des Browsers gelöscht, wenn der Browser geschlossen wird. Wenn Sie beständige Sitzungscookies aktivieren, wird das IVE-Sitzungscookie auf die Festplatte des Clients geschrieben, so dass die IVE-Anmeldeinformationen des Benutzers für die Dauer der IVE-Sitzung gespeichert werden. Die IVE-Sitzungsdauer wird sowohl vom Wert des Leerlaufzeitlimits als auch dem Wert der maximalen Sitzungsdauer bestimmt, die Sie für die Gruppe angeben (siehe Seite 133). Die IVE-Sitzung wird **nicht** beendet, wenn ein Benutzer den Browser schließt. Eine IVE-Sitzung wird erst dann beendet, wenn sich ein Benutzer vom IVE abmeldet. Wenn ein Benutzer das Browserfenster schließt, ohne sich abzumelden, kann jeder

beliebige Benutzer eine andere Instanz desselben Browsers öffnen, um auf das IVE zuzugreifen, ohne gültige Anmeldeinformationen zu senden.

**Wichtig:** Wir empfehlen, diese Funktion nur für eine Autorisierungsgruppe zu aktivieren, deren Mitglieder den Zugriff auf Anwendungen benötigen, für die IVE-Anmeldeinformationen erforderlich sind, sowie sicherzustellen, dass sich diese Benutzer der Bedeutung der Abmeldung aus dem IVE nach Abschluss der Sitzung bewusst sind. Wenn Sie vor dem Fortfahren weitere Informationen benötigen, wenden Sie sich an den Neoteris Support unter [support@neoteris.com](mailto:support@neoteris.com).

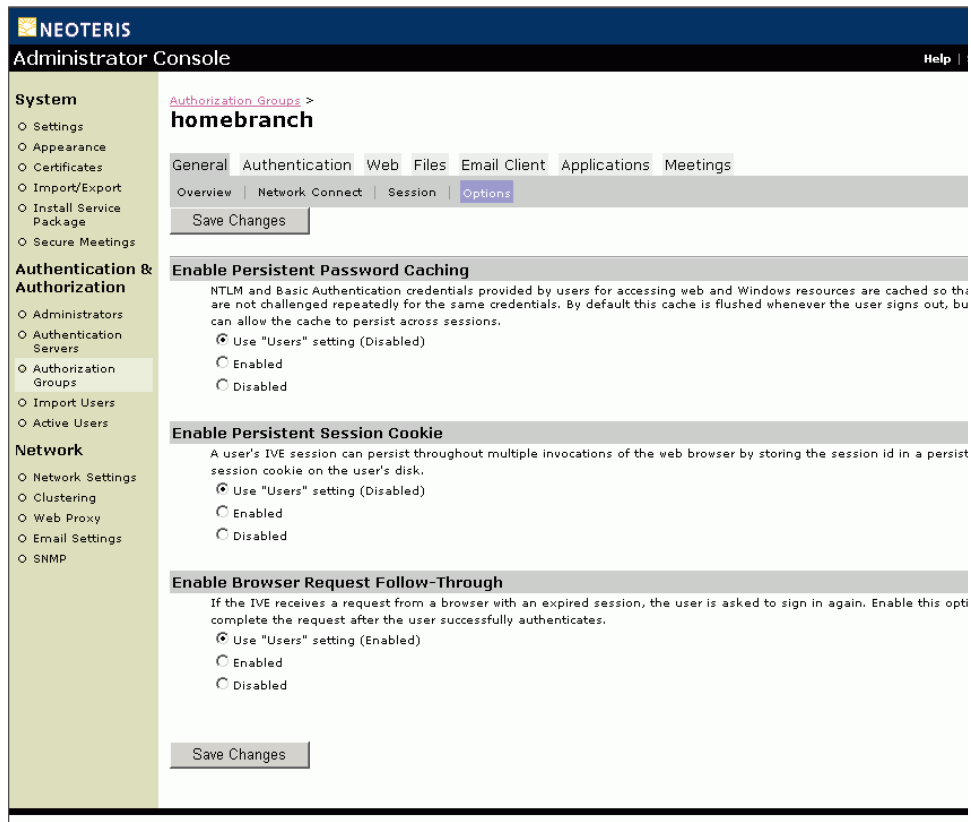


Abbildung 58: Authentication & Authorization > GroupName > General > Options



## Authentication > Unterregisterkarte „Authentication Server“

### ☑ Überprüfen der Zuordnungen von Servern zu Gruppen

Auf dieser Registerkarte können Sie überprüfen, welche Authentifizierungsserver Benutzer einer Autorisierungsgruppe zuordnen. Auf dieser Registerkarte werden alle Instanzen aufgeführt, die der ausgewählten Autorisierungsgruppe derzeit Benutzer zuordnen.

#### So überprüfen Sie die Autorisierungsgruppenzuordnungen des Authentifizierungsservers

1. Wählen Sie in der Administratorkonsole das Menü **Authentication & Authorization > Authorization Groups** und anschließend eine Gruppe aus.
2. Wählen Sie aus den Gruppenregisterkarten **Authentication > Authentication Server**.

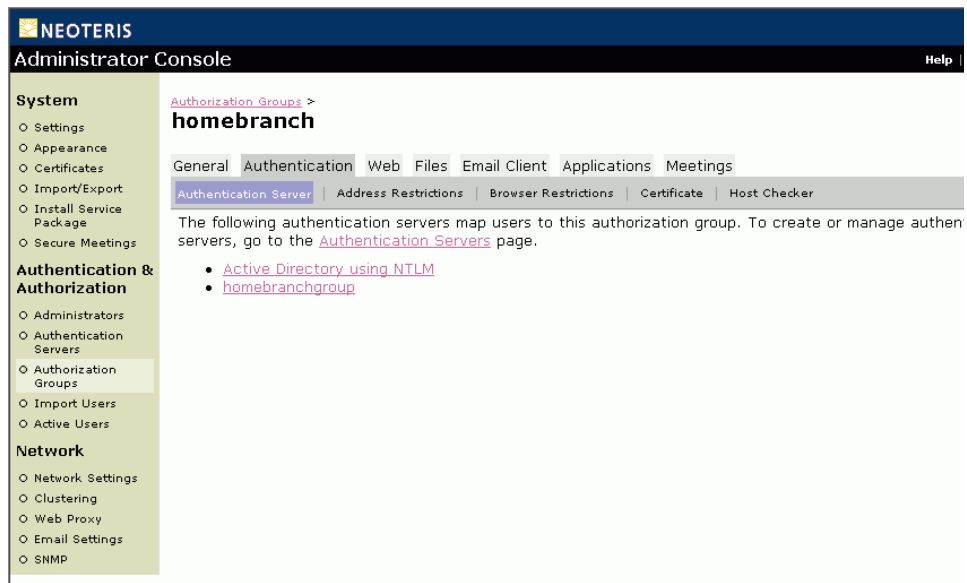


Abbildung 59: Authentication & Authorization > Authorization Groups > GroupName > Authentication > Authentication Server

## Authentication > Unterregisterkarte „Address Restrictions“

### ☒ Einschränken der möglichen IP-Adressen für die Benutzeranmeldung

Auf dieser Registerkarte können Sie den Benutzerzugriff auf die Autorisierungsgruppe einschränken, indem Sie die IP-Adressen festlegen, über die sich Benutzer im IVE anmelden können.

#### So schränken Sie die IP-Adressen ein, über die sich Benutzer anmelden können

1. Wählen Sie in der Administratorkonsole das Menü **Authentication & Authorization > Authorization Groups** und anschließend eine Gruppe aus.
2. Wählen Sie aus den Gruppenregisterkarten **Authentication > Address Restrictions** aus.
3. Wählen Sie eine der folgenden Optionen aus:
  - **Users can sign in from any IP address**, um es den Gruppenmitgliedern zu ermöglichen, sich über jede beliebige IP-Adresse anzumelden. Beachten Sie, dass Sie diese Option auch dann auswählen sollten, wenn die Benutzergruppe für die Anmeldung von Mitgliedern über beliebige IP-Adressen konfiguriert ist. Somit stellen Sie sicher, dass die Gruppenmitglieder sich auch bei Änderungen der Benutzergruppeneinstellung weiterhin von jeder IP-Adresse aus anmelden können.
  - **Users can only sign in from the following IP addresses**, um einzuschränken, über welche IP-Adressen sich die Mitglieder der Gruppe anmelden können. Wenn Sie diese Option auswählen, geben Sie unbedingt die entsprechenden IP-Adressen an, da andernfalls die Anmeldung für Benutzer von keinem Standort aus mehr möglich ist.
4. Wenn Sie es Benutzern ermöglichen möchten, sich über den externen Port anzumelden, klicken Sie auf **Enable**.
5. Klicken Sie auf **Save Changes**.

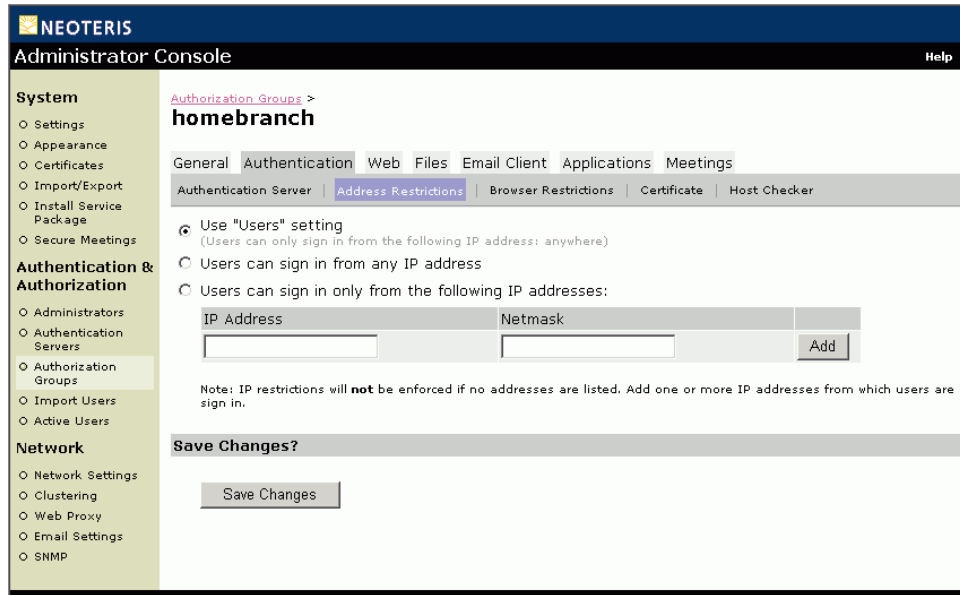


Abbildung 60: Authentication & Authorization > Authorization Groups > GroupName > Authentication > Address Restrictions

## Authentication > Unterregisterkarte „Browser Restrictions“

### ☒ Einschränken der möglichen Browser für die Benutzeranmeldung

Auf dieser Registerkarte können Sie angeben, über welche Webbrowser ein Benutzer auf das IVE zugreifen kann. Wenn ein Benutzer versucht, sich im IVE über einen nicht unterstützten Browser anzumelden, schlägt der Anmeldeversuch fehl, und es wird in einer Meldung angezeigt, dass ein nicht unterstützter Browser verwendet wird. Verwenden Sie diese Zugriffssteuerung, um sicherzustellen, dass sich Benutzer im IVE über Browser anmelden, die mit Firmenanwendungen kompatibel oder von Firmensicherheitsrichtlinien zugelassen sind.

---

**Hinweis:** Das Feature zur Browsereinschränkung dient nicht als strikte Zugriffssteuerung, da die Zeichenfolgen für Benutzer-Agenten des Browsers von einem technischen Benutzer geändert werden können. Es dient als beratende Zugriffssteuerung für normale Nutzungsszenarien.

---

### So geben Sie die Browserzugriffssteuerung an

1. Wählen Sie in der Administratorkonsole das Menü **Authentication & Authorization > Authorization Groups** und anschließend eine Gruppe aus.
2. Wählen Sie aus den Gruppenregisterkarten **Authentication > Browser Restrictions** aus.
3. Wählen Sie die entsprechende Option aus, und klicken Sie dann auf **Save Changes**. Folgende Optionen stehen zur Verfügung:
  - **Use Users group settings**  
Wendet die Einstellungen der Benutzergruppe an.
  - **Users can sign in from any browser**  
Ermöglicht es Benutzern, sich über alle unterstützten Webbrowser anzumelden.
  - **Users can only sign in from the specified browsers**  
Ermöglicht es Ihnen, Regeln für die Browserzugriffssteuerung festzulegen. So erstellen Sie eine Regel
    - 1 Geben Sie im Feld **User-agent string pattern** eine Zeichenfolge im Format `*<browser_string>*` ein. Dabei ist das Zeichen `*` (Sternchen) ein optionales Zeichen, das für die Übereinstimmung mit einem beliebigen Zeichen verwendet wird. Bei `<browser_string>` handelt es sich um ein Muster, bei dem die Groß- und Kleinschreibung beachtet wird, und das mit einer Teilzeichenfolge im vom Browser gesendeten „user-agent“-Header übereinstimmen muss.
    - 2 Wählen Sie entweder **Allow** aus, um es Benutzern zu ermöglichen, sich über jeden Browser anzumelden, dessen „user-agent“-Header die Teilzeichenfolge `<browser_string>` enthält, oder wählen Sie **Deny** aus, wenn die Anmeldung für Benutzer nicht über jeden Browser möglich sein soll, dessen „user-agent“-Header die Teilzeichenfolge `<browser_string>` enthält.

#### Hinweise:

- Regeln werden der Reihenfolge nach angewendet, d. h., die erste übereinstimmende Regel wird angewendet.
- Bei Literalzeichen in Regeln wird die Groß- und Kleinschreibung beachtet, Leerzeichen sind dabei zulässig.
- Standardmäßig lautet die letzte Regel **\* Allow**, d. h., Benutzer können sich über alle anderen Browser anmelden. Ändern Sie den Befehl in **Deny**, damit sich Benutzer nur über durch andere Regeln angegebene Browser anmelden können.

### Beispiele:

- Die Zeichenfolge \*Netscape\* findet für alle Zeichenfolgen für Benutzer-Agenten eine Übereinstimmung, die die Teilzeichenfolge Netscape enthält.
- Der folgende Regelsatz ermöglicht es Benutzern nur, sich über Internet Explorer 5.5x oder Internet Explorer 6.x anzumelden. In diesem Beispiel werden einige wichtige andere Browser als Internet Explorer berücksichtigt, die die Teilzeichenfolge „MSIE“ im „user-agent“-Header senden:

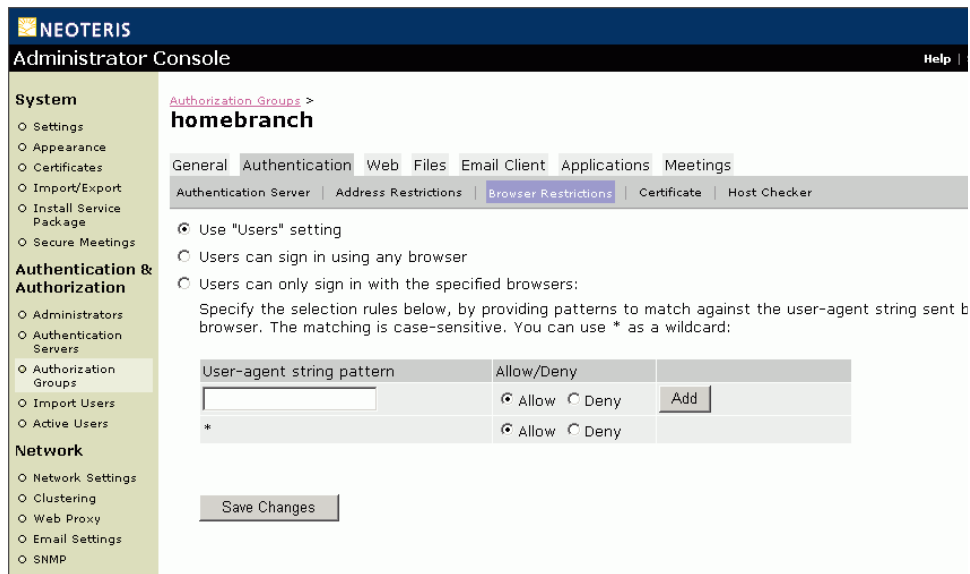
\*Opera\***Deny**

\*AOL\***Deny**

\*MSIE 5.5\***Allow**

\*MSIE 6.\***Allow**

\* **Deny**



**Abbildung 61: Authentication & Authorization > Authorization Groups > GroupName > Authentication > Browser Restrictions**

## Authentication > Unterregisterkarte „Certificate“

### ☒ Festlegen, dass Clientcomputer über ein gültiges Zertifikat verfügen müssen

Auf dieser Registerkarte können Sie angeben, dass Clientcomputer, auf denen sich Benutzer anmelden, über ein gültiges clientseitiges Zertifikat verfügen müssen. Wenn Sie dieses Feature verwenden, stellen Sie sicher, dass Sie ein Stammzertifikat importieren, um das clientseitige Zertifikat zu überprüfen. Weitere Informationen finden Sie unter „Importieren eines Stammzertifikats zur Überprüfung eines clientseitigen Zertifikats“ auf Seite 52. Vergewissern Sie sich zur Optimierung der Sicherheit dieses Features, dass die Clienteinstellungen eines Benutzers so festgelegt sind, dass der Benutzer bei jeder Anmeldung ein Kennwort eingeben muss. In der Standardeinstellung wird bei einigen Browserversionen das Zertifikatkennwort gespeichert, d. h. der Benutzer wird nach Installation des Zertifikats nicht zur Eingabe dieser zusätzlichen Anmeldeinformationen aufgefordert.

### So legen Sie fest, dass Clientcomputer über ein gültiges clientseitiges Zertifikat verfügen müssen

1. Wählen Sie in der Administratorkonsole das Menü **Authentication & Authorization > Authorization Groups** und anschließend eine Gruppe aus.
2. Wählen Sie aus den Gruppenregisterkarten **Authentication > Certificate** aus.
3. Wählen Sie die entsprechende Option aus, und klicken Sie dann auf **Save Changes**. Folgende Optionen stehen zur Verfügung:
  - **Use Users group settings**  
Wendet die Einstellungen der Benutzergruppe an.
  - **Users do NOT require clientside certificate for authentication**  
Diese Einstellung ermöglicht es Mitgliedern der Gruppe, sich von einem Client anzumelden, der nicht über ein clientseitiges Zertifikat verfügt.
  - **Users require clientside certificate with following attributes for authentication**  
Bei dieser Einstellung müssen Mitglieder der Gruppe über ein clientseitiges Zertifikat verfügen. Um den Zugriff noch weiter einzuschränken, können Sie für die Gruppe eindeutige Attribut-Wert-Paare für das Zertifikat festlegen.

**Hinweise:**

- Alle X.509-DN-Attribute (Distinguished Name) werden unterstützt (z. B. C, CN, L, O, OU).
- Bei den Attribut- und Wertefeldern wird die Groß- und Kleinschreibung nicht beachtet.
- Definieren Sie für jedes Attribut nur einen Wert. Wenn Sie mehrere Werte angeben, kann das clientseitige Zertifikat möglicherweise nicht korrekt anhand des Stammzertifikats authentifiziert werden.

The screenshot displays the Neoteris Administrator Console interface. On the left is a navigation menu with categories: System, Authentication & Authorization, and Network. The 'Authentication & Authorization' section is expanded, showing 'Authorization Groups' as the selected item. The main content area shows the configuration for the 'homebranch' group. It includes tabs for General, Authentication, Web, Files, Email Client, Applications, and Meetings. The 'Authentication' tab is active, showing sub-tabs for Authentication Server, Address Restrictions, Browser Restrictions, Certificate, and Host Checker. The 'Certificate' sub-tab is selected, displaying the 'SSL Client-side Digital Certificate Authentication' settings. Three radio button options are present: 'Use "Users" setting' (selected), 'Users do NOT require a client-side certificate for authentication', and 'Users require a client-side certificate with following attributes for authentication'. Below these is a table with columns 'Certificate Field' and 'Field Value', and an 'Add' button. A note at the bottom states: 'Certificate Field is a component of a X.509 Distinguished Name: C, ST, L, O, OU, CN, T, I, G, S, D, UID, or Email Field and its value are case insensitive.' At the bottom of the configuration area is a 'Save Changes?' section with a 'Save Changes' button.

**Abbildung 62: Authentication & Authorization > Authorization Groups > GroupName > Authentication > Certificate**

## Authentication > Unterregisterkarte „Host Checker“

Mit der Hostprüfung werden auf Hosts, die mit dem IVE eine Verbindung herstellen, Endpunktsicherheitsprüfungen durchgeführt. Wenn dieses Feature für eine Gruppe aktiviert wird, wird vom IVE ein transparentes ActiveX-Steuerelement heruntergeladen, mit dem der Client des Benutzers auf angegebene Eigenschaften von Anwendungen für die Endpunktsicherheit überprüft wird. Wenn die erforderlichen Eigenschaften nicht gefunden werden, kann der Benutzer nicht auf die IVE-Startseite zugreifen.

Das IVE verwendet drei Methoden, um Hosts auf Anwendungen für die Endpunktsicherheit zu überprüfen:

- **AYT-Integration**

Durch das ActiveX-Steuerelement wird die AYT-API (Are You There) der angegebenen Anwendung für die Endpunktsicherheit aufgerufen und der Rückgabewert überprüft, um festzustellen, ob die Anwendung gefunden wurde und ordnungsgemäß funktioniert. Das IVE unterstützt derzeit AYT-Aufrufe der folgenden Anwendungen:

- Sygate Firewall AYT
- Sygate Secure Agent AYT
- Zone Labs AYT

- **NHC-API-Integration**

Mit der Hostprüfung von Neoteris (NHC-API) können Sie eine benutzerdefinierte DLL schreiben, mit der überprüft wird, ob eine Software für Endpunktsicherheit eines Drittanbieters auf dem Clientcomputer vorhanden ist. Sie müssen diese DLL auf jedem Clientcomputer installieren. Um weitere Informationen zu erhalten, wenden Sie sich an den Neoteris-Support.

- **Attributüberprüfung**

Das ActiveX-Steuerelement sucht nach den Spuren der angegebenen Anwendung, einschließlich Registrierungseinträge und Daemonvorgang.

Wenn ein Benutzer seine Anmeldeinformationen auf der IVE-Anmeldeseite eingibt, wird während des Herunterladens des ActiveX-Steuerelements eine Seite mit der Meldung „Starting Host Checker“ angezeigt. Daraufhin wird der Client durch die Hostprüfung auf Software für die Endpunktsicherheit überprüft, indem die in der Administratorkonsole angegebene Methode verwendet wird. Wenn die Überprüfung durch die Hostprüfung fehlschlägt, wird im IVE eine Fehlermeldung angezeigt und der Benutzer auf die Anmeldeseite umgeleitet.

Das IVE wartet 120 Sekunden darauf, dass die Hostprüfung feststellt, ob der Client über die benötigte Software für die Endpunktsicherheit verfügt. Nach Ablauf dieser Zeit wird im IVE eine Fehlermeldung angezeigt und der Benutzer



auf die Anmeldeseite umgeleitet. Unabhängig von Erfolg oder Fehlschlagen bleibt die Hostprüfung auf dem Client im Verzeichnis „C:\Programme\Neoteris\Host Checker“. Das Steuerelement kann von Benutzern manuell deinstalliert werden, indem in diesem Verzeichnis die Datei „uninstall.exe“ ausgeführt wird. In diesem Verzeichnis ist auch eine Protokolldatei enthalten, die bei jedem Ausführen der Hostprüfung neu erstellt wird.

## ☑ Durchführen einer clientseitigen Überprüfung der Software für die Endpunktsicherheit

Verwenden Sie diese Registerkarte zum Aktivieren der IVE-Hostprüfung, und geben Sie die Methode an, mit der das Steuerelement für die ActiveX-Hostprüfung überprüft, ob der Client über die benötigte Software für die Endpunktsicherheit verfügt.

---

**Hinweis:** Die Hostprüfung überprüft nicht, ob die benötigte Software für die Endpunktsicherheit ausgeführt wird. Auch das Verhalten dieser Software wird nicht überprüft. Verwenden Sie die Hostprüfung als Tool zur Durchsetzung von Richtlinien zum Verwalten der Endpunktsicherheit.

---

### So führen Sie eine clientseitige Überprüfung der Software für die Endpunktsicherheit durch

1. Wählen Sie in der Administratorkonsole das Menü **Authentication & Authorization > Authorization Groups** und anschließend eine Gruppe aus.
2. Wählen Sie aus den Gruppenregisterkarten **Authentication > Host Checker** aus.

Benutzerdefinierte Autorisierungsgruppen erben standardmäßig die Einstellungen der Benutzergruppe. Klicken Sie zum Festlegen benutzerdefinierter Einstellungen auf **Use custom settings** und anschließend auf **Update**.

3. Klicken Sie unter **Host Checking** auf **Enabled**.
4. Wählen Sie unter **Host Checking Method** eine der folgenden Optionen aus:
  - **Sygate Personal Firewall AYT**  
Zur Verwendung dieser Option muss Sygate Personal Firewall auf dem Clientcomputer installiert sein.
  - **Sygate Secure Agent AYT**  
Zur Verwendung dieser Option muss Sygate Secure Agent auf dem Clientcomputer installiert sein.

- **Zone Labs AYT**

Zur Verwendung dieser Option muss Zone Alarm Pro oder ein Integrity-Produkt auf dem Clientcomputer installiert sein.

- **Other endpoint security applications**

Zur Verwendung dieser Option müssen Sie mit dem Neoteris-Support zusammenarbeiten, um eine DLL eines Drittanbieters zu erstellen, die die NHC-API (Neoteris Host Checker, Hostprüfung von Neoteris) implementiert. Daraufhin müssen Sie diese DLL auf den entsprechenden Clientcomputern installieren und im Feld **DLL path** den Pfad zu der DLL angeben. Wenn die Hostprüfung auf dem Clientcomputer ausgeführt wird, wird die NHC AYT-Funktion in der DLL aufgerufen.

- **Client attribute checking**

Zur Verwendung dieser Option müssen Sie drei Informationen angeben, durch die die Anwendung für die Endpunktsicherheit bezeichnet werden:

- Ein Registrierungsstammschlüssel—Wählen Sie einen Stammschlüssel aus der Dropdownliste aus.
- Ein Registrierungsteilschlüssel—Geben Sie den Pfad zum Anwendungsordner ein. Dem Pfadnamen muss kein „\“ (umgekehrter Schrägstrich) vorangestellt werden.
- Der Prozessname der Anwendung—Dieser Name ist der Prozessname, der im Task-Manager von Windows angezeigt wird.

5. Geben Sie unter **Additional Options** das Intervall in Minuten an, in dem die Hostprüfung ausgeführt werden soll. Die Hostprüfung wird 120 Sekunden lang ausgeführt. Dann wird vom IVE eine Fehlermeldung angezeigt, der Benutzer aus dem IVE entfernt und auf die Anmeldeseite umgeleitet.

---

**Hinweis:** Das IVE wird nicht benachrichtigt, wenn die Anwendung für die Endpunktsicherheit beendet wird (durch Absturz oder Fremdeinwirkung).

---

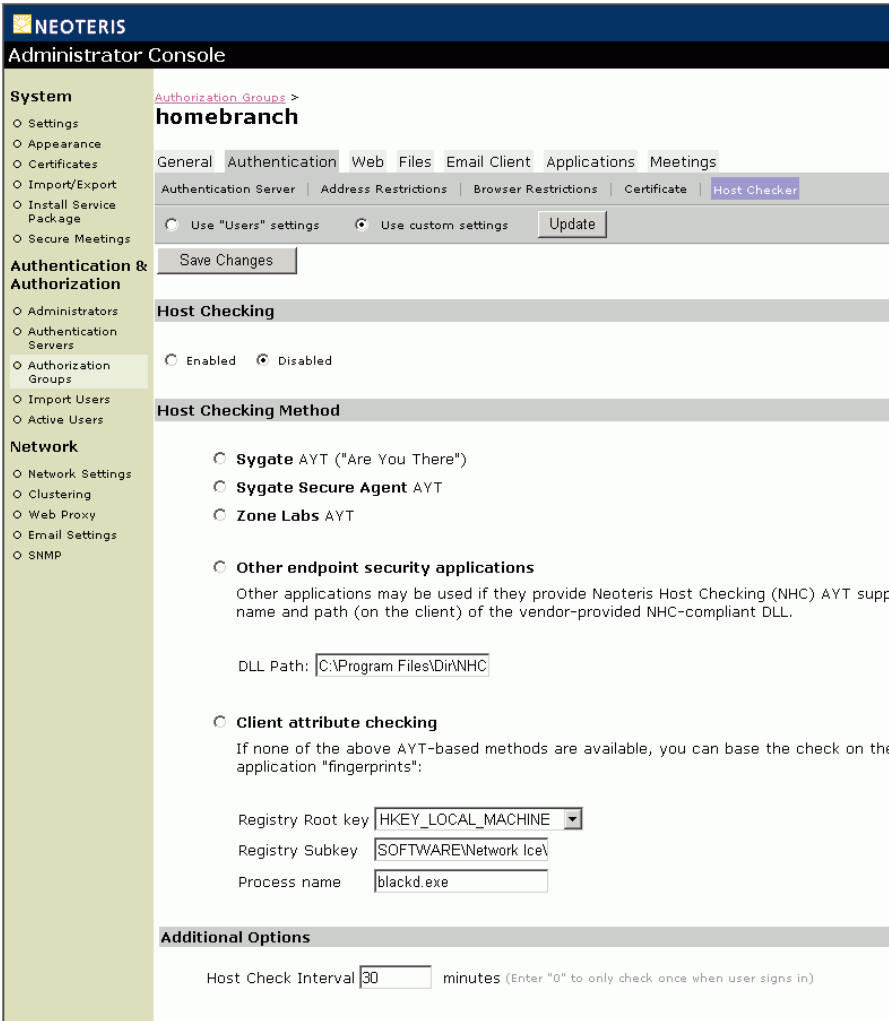


Abbildung 63: Authentication & Authorization > Authorization Groups > GroupName > Authentication > Host Checker

## Web > Unterregisterkarte „General“

### ☒ Festlegen von allgemeinen Einstellungen für Webbrowsing

Auf dieser Registerkarte können Sie Benutzeroptionen für Webbrowsing angeben, z. B. die Möglichkeit zum Eingeben von URLs und zum Erstellen von Lesezeichen.

#### So legen Sie allgemeine Einstellungen für Webbrowsing fest

1. Wählen Sie in der Administratorkonsole das Menü **Authentication & Authorization > Authorization Groups** und anschließend eine Gruppe aus.
2. Wählen Sie aus den Gruppenregisterkarten **Web > General** aus.
3. Wählen Sie die Einstellungen für die jeweiligen Optionen aus, und klicken Sie anschließend auf **Save Changes**. Folgende Optionen stehen zur Verfügung:

- **Enable Web Browsing**

Die Webbrowsingoptionen werden zusammen mit der für die Autorisierungsgruppe definierte Richtlinie für die Webzugriffssteuerung (Seite 158) verwendet. Folgende Optionen stehen zur Verfügung:

- **Users can enter URLs, add bookmarks, and view group bookmarks**

Diese Option ermöglicht es den Benutzern, persönliche Lesezeichen für URLs auf verfügbaren Webservern zu durchsuchen und zu erstellen. Die Benutzer können auch zu vom Administrator definierten Lesezeichen auf verfügbaren Webserver wechseln.

- **Users can enter URLs and view group bookmarks**

Diese Option ermöglicht es den Benutzern, zu URLs und vom Administrator definierten Lesezeichen auf verfügbaren Webservern zu wechseln.

- **Users can view group bookmarks only**

Diese Option ermöglicht es den Benutzern lediglich, zu vom Administrator definierten Lesezeichen auf verfügbaren Webservern zu wechseln.

- **Web browsing disabled**

Bei dieser Option können die Benutzer keine Webressourcen durchsuchen. Verwenden Sie diese Option, wenn Sie die Zugriffsmöglichkeiten schnell ändern müssen, die Richtlinien für Webressourcen sowie Zugriffssteuerungslisten jedoch erhalten bleiben sollen. Wenn Sie diese Option auswählen, werden auf der IVE-Startseite keine Elemente für Webbrowsing mehr angezeigt.

- **Enable Java Applet Support**

Aktivieren Sie dieses Feature, um es den Benutzern zu ermöglichen, zu Webseiten mit clientseitigen Java-Applets zu wechseln. Der IVE-Server wird für den Anwendungsserver wie ein Browser über SSL behandelt. Das IVE verarbeitet alle durch ein Java-Applet initiierten HTTP-Anforderungen und TCP-Verbindungen transparent und verarbeitet signierte Java-Applets. Wenn Sie dieses Feature aktivieren, können die Benutzer Java-Applets starten und Anwendungen ausführen, die als clientseitige Java-Applets implementiert wurden, z. B. den VNC-Java-Client (Virtual Computing), Citrix NFuse Java-Client, WRQ Reflections Web-Client und Lotus WebMail. Folgende Optionen sind für dieses Feature verfügbar:

- **Enabled, with full network connectivity**

Durch diese Option können signierte Java-Applets eine Verbindung mit jedem beliebigen Server aufbauen.

- **Enabled, with access control (see Java Access Control)**

Durch diese Option können Sie angeben, mit welchen Servern und Ports ein Applet eine Verbindung herstellen kann.

- **Limited (HTTP enabled, but no socket connectivity)**

Durch diese Option können Java-Applets eine Verbindung mit Servern aufbauen, die nur HTTP oder HTTPS verwenden.

- **Disabled**

Diese Option verhindert, dass das IVE Java-Applets bedient. Wenn ein Benutzer zu einer Webseite mit einem Java-Applet wechselt, wird auf der Webseite an der Stelle, an der normalerweise das Java-Applet angezeigt wird, ein graues Feld mit folgender Meldung angezeigt: „Java applet support is disabled on the secure gateway.“

### Hinweise

- Nicht signierte Applets können nur mit dem Host eine Verbindung herstellen, von dem sie heruntergeladen wurden.
  - Wenn Sie die Unterstützung für Java-Applets deaktivieren, den Durchgangssproxy (Seite 150) jedoch als Vermittler einer Anwendung konfigurieren, die Applets bedient, bedient das IVE Applets ohne Vermittlung.
- **Enable Persistent (Web) Cookies**

Standardmäßig löscht der Neoteris IVE-Server Webcookies, die während einer Benutzersitzung gespeichert wurden. Damit eine Gruppe das Navigieren im Web anpassen kann, ändern Sie diese Option, so dass beständige Cookies beibehalten werden. Ein Benutzer kann Cookies über die Seite **Advanced Preferences** löschen.

- **Enable Selective Rewriting**

Mit dieser Option können Sie eine Liste von Hosts definieren, für die das IVE Inhalte und Ausnahmen von dieser Liste vermitteln soll. Standardmäßig vermittelt das IVE alle Benutzeranforderungen für Webhosts, sofern Sie das IVE nicht zum Verarbeiten von Anforderungen für bestimmte Hosts mit Hilfe eines anderen Mechanismus konfiguriert haben, z. B. Secure Application Manager.

Verwenden Sie diese Option, wenn das IVE den Datenverkehr von Websites vermitteln soll, die sich außerhalb des Firmennetzwerks befinden, z. B. „yahoo.com“, oder wenn das IVE keinen Datenverkehr für Client-/Serveranwendungen vermitteln soll, die Sie als Webressourcen bereitgestellt haben, z. B. Microsoft OWA (Outlook Web Access).

Informationen zum Konfigurieren von Hosts und Ausnahmen für selektives Neuschreiben finden Sie unter „Konfigurieren von Hosts für die Option zum selektiven Neuschreiben“ auf Seite 152.

- **Enable Pass-Through Proxy**

Mit dieser Option können Sie Webanwendungen angeben, für die das IVE eine minimale Vermittlung durchführt. Anders als die herkömmliche Antwortproxymfunktion, bei der ebenfalls nur selektive Teile einer Serverantwort neu geschrieben werden, jedoch sowohl Netzwerkänderungen als auch komplexe Konfigurationen vorgenommen werden müssen, müssen Sie für diese Option lediglich Anwendungsserver angeben sowie die Art, in der das IVE Clientanforderungen an diese Anwendungsserver empfängt:

- **Via an IVE port**

Wenn Sie eine Anwendung zur Vermittlung für den Durchgangssproxy angeben, geben Sie einen Port an, an dem das IVE Clientanforderungen an den Anwendungsserver abfragen soll. Wenn das IVE eine Clientanforderung für den Anwendungsserver empfängt, leitet es die Anforderung an den angegebenen Anwendungsserverport weiter.

Wenn Sie diese Option auswählen, müssen Sie bei Ihrer Firmenfirewall den Datenverkehr für den angegebenen IVE-Port freigeben.

- **Via external DNS resolution**

Wenn Sie eine Anwendung zur Vermittlung für den Durchgangssproxy angeben, geben Sie einen Alias für den Hostnamen des Anwendungsservers ein. Für diesen Alias müssen Sie einen Eintrag im externen DNS vornehmen, der für das IVE aufgelöst wird. Wenn das IVE eine Clientanforderung für den Alias empfängt, leitet er die Anforderung an den für den Anwendungsserver angegebenen Port weiter.

Diese Option bietet sich an, wenn in Ihrem Unternehmen restriktive Richtlinien für das Öffnen von Firewallports zum Zugriff auf das IVE bestehen. Wenn Sie diese Option verwenden, ist es empfehlenswert, dass jeder Hostnamenalias dieselbe Domänenteilzeichenfolge enthält wie der IVE-Hostname und dass Sie in folgendem Format ein Serverzertifikat mit Platzhalter in das IVE hochladen: \*.domaene.com.

Wenn der IVE beispielsweise iveserver.ihrefirma.com lautet, muss der Hostnamenalias im Format anwserver.ihrefirma.com und mit Platzhalter im Format \*.ihrefirma.com angegeben werden. Wenn Sie kein Zertifikat mit Platzhalter verwenden, stellt der Browser eines Clients eine Warnung zu einer Zertifikatsnamenüberprüfung aus, wenn ein Benutzer zu einem Anwendungsserver wechselt, da der Hostnamenalias des Anwendungsservers nicht mit dem Zertifikatsdomänennamen übereinstimmt. Durch dieses Verhalten wird ein Benutzer jedoch nicht daran gehindert, auf den Anwendungsserver zuzugreifen.

### Beispiele

Wenn das IVE den Namen iveserver.IhreFirma.com hat und Sie über einen Oracle-Server bei oracle.companynetwork.net:8000 verfügen, könnten Sie diese Anwendungsparameter bei der Angabe eines IVE-Ports angeben:

**Server:** oracle.companynetwork.net

**Port:** 8000

**IVE Port:** 11000

Wenn das IVE Datenverkehr vom Oracle-Client empfängt, der an iveserver.IhreFirma.com:11000 gesendet wurde, leitet er den Verkehr an oracle.companynetwork.net:8000 weiter.

Wenn Sie einen Hostnamenalias angeben möchten, können Sie die Anwendung mit folgenden Parametern konfigurieren:

**Server:** oracle.companynetwork.net

**Port:** 8000

**IVE Alias:** oracle.IhreFirma.com

Wenn das IVE Datenverkehr vom Oracle-Client empfängt, der an oracle.IhreFirma.com gesendet wurde, leitet er den Datenverkehr an oracle.companynetwork.net:8000 weiter.

Wenn Sie Clientanforderungen an das IVE basierend auf dem Hostnamenalias weiterleiten, müssen Sie das IVE außerdem dem externen DNS-Server hinzufügen. Diese Option bietet sich an, wenn in Ihrem Unternehmen restriktive Richtlinien für das Öffnen von Firewallports für interne Server oder Server in der DMZ gelten.

Ebenso wie das eigentliche Vermittlungsmodul bietet die Option des Durchgangsproxys eine höhere Sicherheit als Secure Application Manager, da bei Aktivierung für eine Anwendung das IVE dem Client ermöglicht, nur Layer-7-Verkehr an feste Anwendungspoints an das Firmennetzwerk zu senden. Wenn diese Option aktiviert ist, kann das IVE Anwendungen mit Komponenten unterstützen, die nicht mit dem Modul für die Inhaltsvermittlung kompatibel sind, wie Java-Applets in Anwendungen der Oracle E-Business Suite oder Applets, die auf einer nicht unterstützten Java Virtual Machine ausgeführt werden.

---

**Hinweis:** Die Option des Durchgangsproxys kann nur bei Anwendungen verwendet werden, die feste Ports abfragen und bei denen der Client keine direkten Socketverbindungen herstellt.

---

Informationen zum Angeben von Anwendungen, für die das IVE eine minimale Vermittlung durchführt, finden Sie unter „Aktivieren und Angeben von Einstellungen für den Durchgangssproxy“ auf Seite 153.

## ☒ Konfigurieren von Hosts für die Option zum selektiven Neuschreiben

Übersichtsinformationen finden Sie unter „Enable Selective Rewriting“ auf Seite 150.

### So geben Sie die Einstellungen für selektives Neuschreiben an

1. Wählen Sie in der Administratorkonsole das Menü **Authentication & Authorization > Authorization Groups** und anschließend eine Gruppe aus.
2. Wählen Sie aus den Gruppenregisterkarten **Web > General** aus.
3. Wählen Sie unter **Enable Selective Rewriting** den Eintrag **Enabled** aus, und klicken Sie dann auf **Save Changes**.
4. Klicken Sie unter **Enable Selective Rewriting** auf **Selective Rewriting Settings**.
5. Geben Sie unter **Rewrite** alle Hosts an, für die das IVE Inhalt vermitteln soll. Standardmäßig wird ein Sternchen (\*) definiert, was bedeutet, dass jeder Inhalt von einem internen Webhost vermittelt werden soll. Um die Liste **Rewrite** zu ändern, geben Sie ein Hostmuster oder eine Kombination aus IP-Adresse und Netzmaske pro Zeile ein. Mit einem Sternchen können Sie eine Übereinstimmung mit einer beliebigen Teilzeichenfolge einschließlich eines Null-Zeichens erzielen, und mit einem Fragezeichen (?) können Sie ein beliebiges einzelnes Zeichen suchen.



Wenn eine Clientanforderung für einen Host erstellt wird, der nicht in der Liste **Rewrite** enthalten ist, wird im IVE eine Seite angezeigt, die eine Verknüpfung mit der angeforderten Ressource enthält, und Benutzer werden aufgefordert, auf die Verknüpfung zu klicken. Durch diese Verknüpfung wird die Ressource in einem neuen Browserfenster geöffnet, und die Seite, von der die Anforderung ursprünglich durchgeführt wurde, wird weiterhin im IVE angezeigt. Wenn der Benutzer transparent zur Ressource innerhalb des IVE-Browserfensters umgeleitet werden soll, deaktivieren Sie unter **Additional options** das Kontrollkästchen **Open non-rewritten resources in a intermediate page**.

---

**Hinweis:** Wenn Sie dieses Kontrollkästchen deaktivieren, ist es für die Benutzer möglicherweise nicht bemerkbar, dass ihre IVE-Sitzung noch aktiv ist, und dass sie im Browser auf die Schaltfläche **Zurück** klicken müssen, um zum IVE zurückzukehren. Zum Abmelden müssen die Benutzer zum IVE zurückkehren. Wenn sie lediglich das Browserfenster schließen, bleiben die Sitzungen bis zum Ablauf der Sitzungszeitbegrenzung aktiv.

---

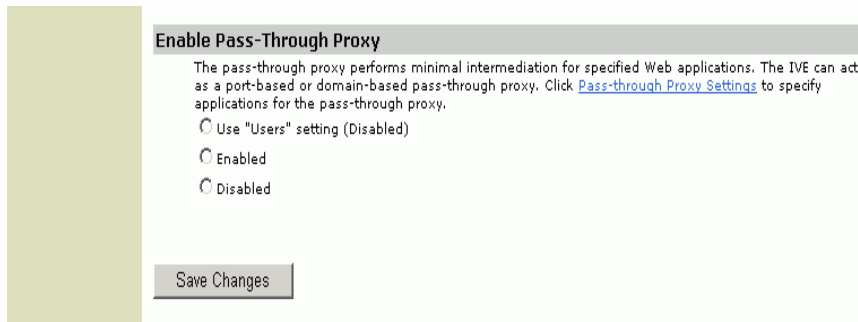
6. Wenn Sie bei bestimmten URLs sicherstellen möchten, dass das IVE als Vermittler fungiert, geben Sie ein URL-Muster ein, das mit dem Host übereinstimmt. Diese Option ist nützlich, wenn Sie sichergehen möchten, dass URLs von Hosts, die für Secure Application Manager konfiguriert wurden, ausschließlich an das Browserfenster des IVE weitergeleitet werden.
7. Klicken Sie auf **Save Changes**.

## ☒ Aktivieren und Angeben von Einstellungen für den Durchgangssproxy

Wenn Sie die Option des Durchgangssproxys aktivieren, müssen Sie zwei Angaben vornehmen:

- Die Webanwendungen, die mit dem Durchgangssproxy vermittelt werden
- Die Art der Überwachung von Clientanforderungen für die Anwendungsserver durch das IVE

Die Option, mit der das IVE Clientanforderungen für den Durchgangsserver überwacht, ist eine systemweite Einstellung. Sie können nicht festlegen, dass das IVE für einige Anwendungsserver Ports überwacht und für andere Anwendungsserver Anforderungen an Aliase überwacht.



**Abbildung 64: Aktivieren des Durchgangsproxys auf der Unterregisterkarte „Users group Web > General“**

Die auf dieser Unterregisterkarte für die Benutzergruppe ausgewählte Option wird auf alle anderen Gruppen angewendet.

Unter „Enable Pass-Through Proxy“ auf Seite 150 finden Sie Übersichtsinformationen und Beispiele, wie das IVE Clientanforderungen überwacht.

### **So aktivieren Sie Anwendungen und geben diese für den Durchgangsproxy an**

1. Wählen Sie in der Administratorkonsole **Authentication & Authorization > Authorization Groups**, und wählen Sie anschließend die Gruppe **Users** aus.
2. Wählen Sie aus den Gruppenregisterkarten **Web > General** aus.
3. Geben Sie unter **Enable Pass-Through Proxy** die Aktivierungsart für die Durchgangsproxyfunktion an:

- **Enabled via an IVE port**

Bei Auswahl dieser Option überwacht das IVE Clientanforderungen für einen Anwendungsserver an einem angegebenen IVE-Port. Wenn das IVE eine Clientanforderung für den Anwendungsserver empfängt, leitet es die Anforderung an den angegebenen Anwendungsserverport weiter.

- **Enabled via external DNS resolution**

Durch Festlegen dieser Option geben Sie einen Alias für den Hostnamen des Anwendungsservers an. Wenn das IVE eine Clientanforderung für den Hostnamenalias des Anwendungsservers empfängt, leitet es die Anforderung an den angegebenen Anwendungsserverport weiter.

Wenn Sie diese Option auswählen, müssen Sie auch den vollständig qualifizierten Domännennamen für das IVE angeben. Der Durchgangsproxy verwendet diese Informationen, um Verknüpfungen auf Sites neu zu schreiben, die für den Anwendungsserver extern sind.

4. Klicken Sie auf der Unterregisterkarte **Web > General** der Benutzergruppe auf **Save Changes** und gehen Sie dann folgendermaßen vor:
  - Wenn Sie mit der Konfiguration der Benutzergruppe fortfahren möchten, klicken Sie auf die Verknüpfung **Pass-Through Proxy Settings**.
  - Wenn Sie eine andere Autorisierungsgruppe konfigurieren möchten, wechseln Sie zurück zur Seite **Authorization Groups**, und gehen Sie dann folgendermaßen vor:
    - 1 Wählen Sie die gewünschte Gruppe aus.
    - 2 Klicken Sie auf die Unterregisterkarte **Web > General**.
    - 3 Klicken Sie unter **Enable Pass-Through Proxy** auf die Verknüpfung **Pass-Through Proxy Settings**.
5. Klicken Sie auf **Add Application**.
6. Geben Sie die erforderlichen Anwendungsinformationen ein:
  - Das Protokoll, das das IVE für die Kommunikation mit dem Anwendungsserver verwenden soll
  - Einen Hostnamen oder eine IP-Adresse für den Anwendungsserver
  - Einen Port vom URL, der für den internen Zugriff auf die Anwendung verwendet wird
  - Entweder ein eindeutiger IVE-Port im Bereich von 11000 bis 11099, an dem das IVE Clientanforderungen erhält oder  
Einen Hostnamenalias für den Anwendungsserver, auf dem das IVE Clientanforderungen erhält
  - Das Verfahren, mit dem das IVE Datenverkehr vermittelt:
    - Neuschreiben von Text, der XML-Code enthält
    - Neuschreiben von Text, der keinen XML-Code enthält

Wenn Sie einen Namen und eine Beschreibung für die Anwendung eingeben, werden diese Informationen in der Liste **Application** anstelle des Hostnamens oder der IP-Adresse des Anwendungsservers angezeigt.
7. Klicken Sie auf **Save Changes**.
8. Wenn Sie in Schritt 3 die Option **Enabled via an IVE port** auswählen, öffnen Sie den Datenverkehr zum IVE-Port, den Sie in der Firmenfirewall für den Anwendungsserver angegeben haben.

---

**Hinweis:** Wenn die Anwendung mehrere Ports überwacht, konfigurieren Sie jeden Anwendungsport als separaten Durchgangssproxeintrag mit einem separaten IVE-Port. Wenn Sie über verschiedene Hostnamen oder IP-Adressen auf den Server zugreifen möchten, konfigurieren Sie jede dieser Optionen einzeln. In diesem Fall können Sie denselben IVE-Port verwenden.

---

9. Wenn Sie **Enabled via external DNS resolution** auswählen, müssen Sie außerdem folgende Aktionen durchführen:
  - 1 Hinzufügen eines Eintrags für jeden Hostnamenalias eines Anwendungsservers im externen DNS, der für das IVE aufgelöst wird.
  - 2 Hochladen eines Serverzertifikats mit Platzhaltern in das IVE (empfohlen). Weitere Informationen zu Zertifikaten mit Platzhaltern finden Sie auf Seite 150.

Unter „Appendix C: Pass-Through Proxy Tips: Oracle Financial 11i“ on page 255 finden Sie Tipps zum Konfigurieren von Oracle Financial 11i und anderen 11i-Anwendungen, die mit der Durchgangsfunktion verwendet werden können.

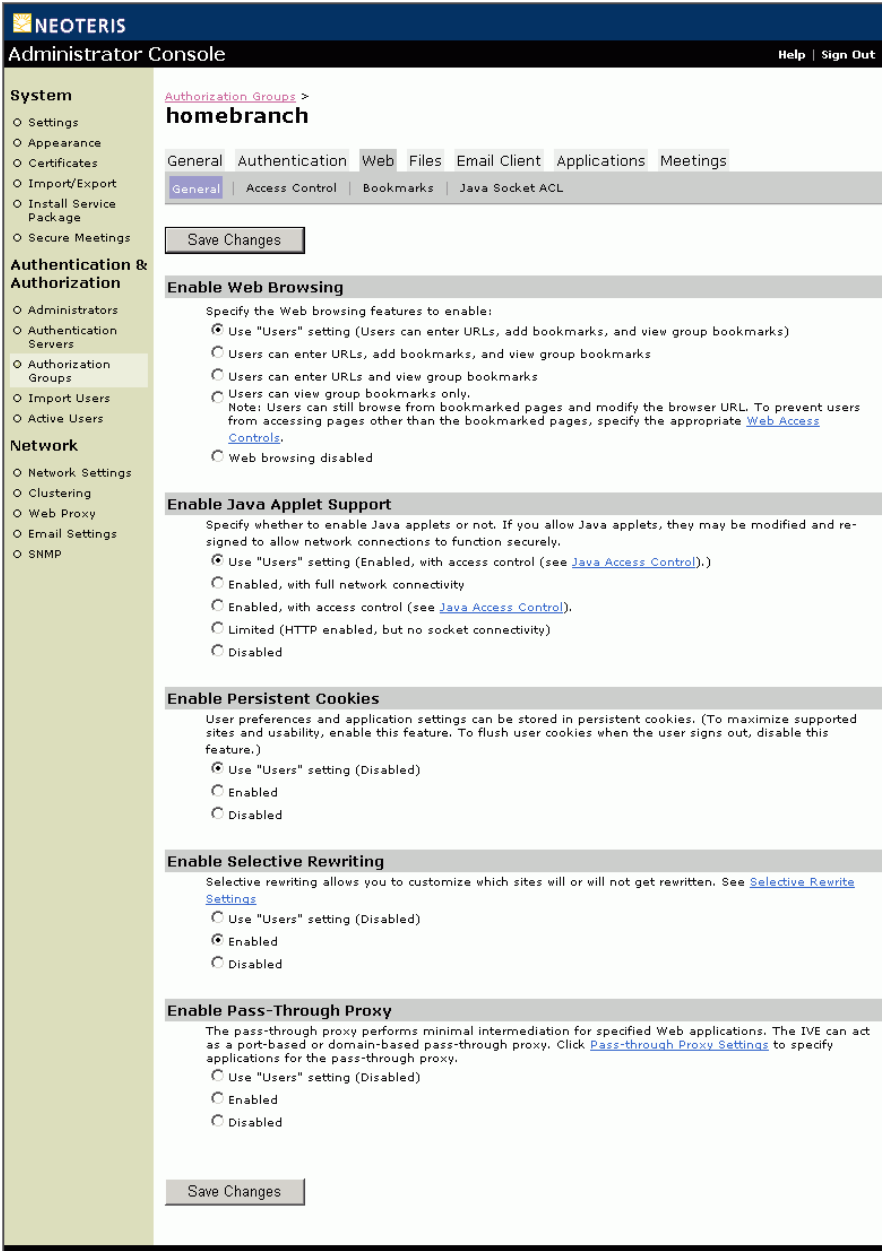


Abbildung 65: Authentication & Authorization > Authorization Groups > GroupName > Web > General

## Web > Unterregisterkarte „Access Control“

### ☒ Zugriffssteuerung für Webressourcen

Sie können angeben, auf welche Webressourcen Benutzer zugreifen können, um eine Verbindung mit dem Internet, Intranet oder Extranet aufzubauen. Es gibt zwei Optionen, um das Standardverhalten festzulegen:

- Eine **open policy** (Standard), mit der der Zugriff auf alle Webressourcen gewährt wird, mit Ausnahme derer in der Liste **Denied Resource**.
- Eine **closed policy**, mit der der Zugriff auf alle Webressourcen verweigert wird, mit Ausnahme derer in der Liste **Allowed Resource**.

Sie können Webressourcen nach URL oder IP-Bereich zulassen bzw. verweigern. Für URLs können Sie die Platzhalter „\*“ und „?“ verwenden, um mehrere Hostnamen und Pfade effektiv anzugeben. Für Ressourcen, die Sie nach Hostnamen angeben, können Sie außerdem entweder HTTP, HTTPS oder beide Protokolle auswählen.

### So steuern Sie den Zugriff auf Webressourcen

1. Wählen Sie in der Administratorkonsole das Menü **Authentication & Authorization > Authorization Groups** und anschließend eine Gruppe aus.
2. Wählen Sie aus den Gruppenregisterkarten **Web > Access Control** aus.  
Benutzerdefinierte Autorisierungsgruppen erben standardmäßig die Einstellungen der Benutzergruppe. Klicken Sie zum Festlegen benutzerdefinierter Einstellungen auf **Use custom settings** und anschließend auf **Update**.
3. Geben Sie im Dropdownfeld **Current Policy** entweder eine geschlossene oder eine offene Richtlinie an, und klicken Sie auf **Change**.

#### Offene Richtlinie

Wenn Sie eine offene Richtlinie auswählen, fügen Sie der Liste **Denied Resources** Ressourcen hinzu, auf die Benutzer nicht zugreifen dürfen:

1. Klicken Sie auf **Deny by Hostname** oder auf **Deny IP Range**.
2. Geben Sie die erforderlichen Informationen ein. Wenn Sie einen Namen und eine Beschreibung für die Ressource eingeben, werden diese Informationen in der Liste **Denied Resources** anstelle des Hostnamens oder der IP-Adresse angezeigt. Beispiel:

Wenn Sie der Liste „Denied Resource“ den Eintrag `http://*Firma.com` hinzufügen, wird einem Benutzer, der `ErsteFirma.com` eingibt, der Zugriff auf die Webseite verweigert.

---

**Hinweis:** Um eine IP-Adresse und einen Port zu sperren, z. B. `http://a.b.c.d:port`, geben Sie die Adresse auf der Seite **Deny Web Resource** ein, und nicht auf der Seite **Deny IP Range**.

---

- 3 Klicken Sie auf **Add Resource** oder auf **Add IP Range**. Die Benutzer können dann nicht mehr auf die Ressource zugreifen, wenn sie sich das nächste Mal im IVE anmelden.

---

**Hinweis:** Die Namen von Webressourcen können in mehrere IP-Adressen oder in unterschiedliche IP-Adressen zu unterschiedlichen Zeiten aufgelöst werden. Wenn Sie unzulässige Ressourcen nach IP-Adresse angeben, stellen Sie sicher, dass Sie alle der Ressource zugeordneten IP-Adressen angeben.

---

### Geschlossene Richtlinie

Wenn Sie eine geschlossene Richtlinie auswählen, fügen Sie der Liste **Allowed Resources** Ressourcen hinzu, auf die die Benutzer zugreifen können:

- 1 Klicken Sie auf **Allow Resource** oder auf **Allow IP Range**.
- 2 Geben Sie die erforderlichen Informationen ein. Wenn Sie einen Namen und eine Beschreibung für die Ressource eingeben, werden diese Informationen in der Liste **Allowed Resources** anstelle des Hostnamens oder der IP-Adresse angezeigt. Beispiel:

Wenn Sie der Liste „Allowed Resource“ den Eintrag `http://*.Firma.com/*.html` hinzufügen, kann ein Benutzer auf alle `html`-Dateien auf dem Server `Firma.com` zugreifen.

- 3 Klicken Sie auf **Add Resource** oder auf **Add IP Range**. Die Benutzer können dann auf die Ressource zugreifen, wenn sie sich das nächste Mal im IVE anmelden.

---

**Hinweis:** Wenn Sie die geschlossene Richtlinie verwenden, stellen Sie sicher, dass die Liste **Allowed Resource** alle Webressourcen enthält, die Inhalt bereitstellen, einschließlich von Ressourcen, die möglicherweise nicht offensichtlich sind, z. B. in den folgenden Fällen:

- Bilder werden von einem anderen Server abgerufen
- Hyperlinks verweisen auf Inhalte auf anderen Servern
- Der Server leitet Anforderungen an einen anderen Server um

Damit das Webbrowsing beim Verwenden einer geschlossenen Richtlinie ordnungsgemäß funktioniert, müssen alle diese Ressourcen in der Liste **Allowed Resource** aufgeführt werden.

---

Zusätzliche Aufgaben

- Um eine Ressource in der Liste der zugelassenen oder verweigerten Ressourcen zu bearbeiten, klicken Sie auf die entsprechende Verknüpfung.
- Um eine Ressource zu löschen, aktivieren Sie das Kontrollkästchen neben dem jeweiligen Namen, und klicken Sie dann auf **Delete**.

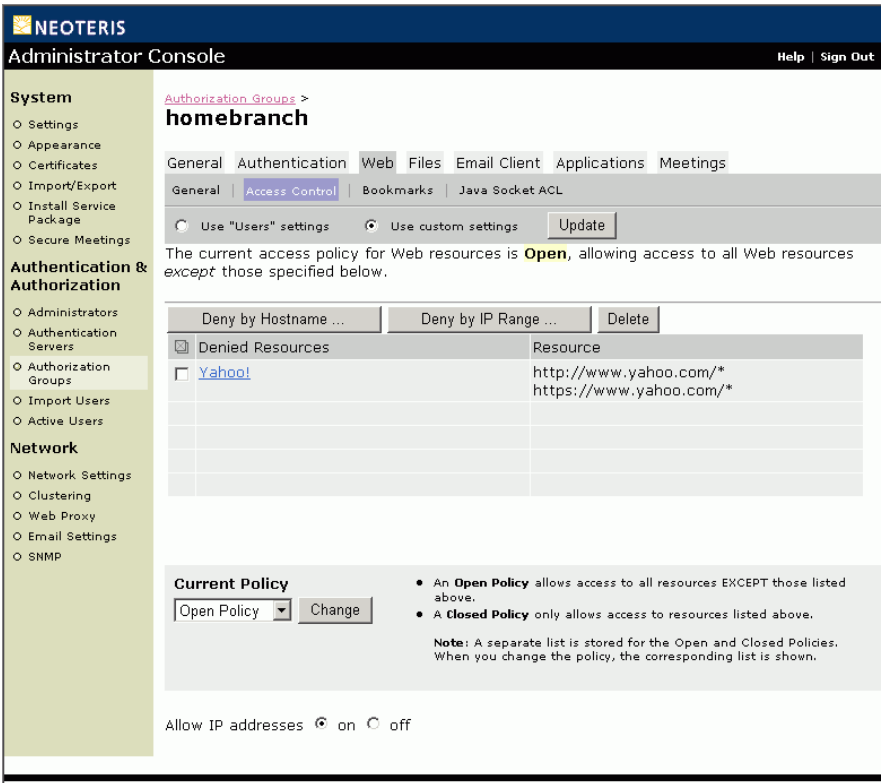


Abbildung 66: Authentication & Authorization > Authorization Groups > GroupName > Web > Access Control



## Web > Unterregisterkarte „Bookmarks“

### ☒ Erstellen von Lesezeichen für Webressourcen

Auf dieser Registerkarte können Sie Weblesezeichen erstellen, die auf der IVE-Startseite angezeigt werden. Sie können den IVE-Benutzernamen eines Benutzers im URL-Pfad einfügen, um bei Einzelanmeldung den Zugriff auf Back-End-Webanwendungen zu ermöglichen.

#### So erstellen Sie ein Weblesezeichen

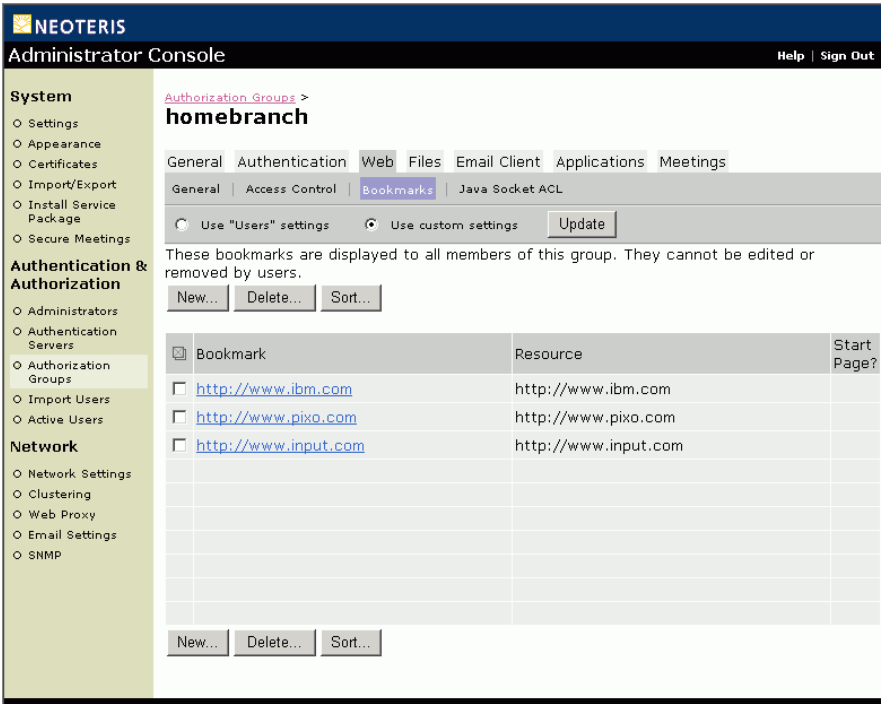
1. Wählen Sie in der Administratorkonsole das Menü **Authentication & Authorization > Authorization Groups** und anschließend eine Gruppe aus.
2. Wählen Sie aus den Gruppenregisterkarten **Web > Bookmarks** aus.  
Benutzerdefinierte Autorisierungsgruppen erben standardmäßig die Einstellungen der Benutzergruppe. Klicken Sie zum Festlegen benutzerdefinierter Einstellungen auf **Use custom settings** und anschließend auf **Update**.
3. Klicken Sie zum Erstellen des Lesezeichens auf **New**:
4. Geben Sie die Einstellungen für das Lesezeichen an:
  - 1 Geben Sie die erforderlichen Informationen ein. Wenn Sie den Benutzernamen des Benutzers einfügen möchten, geben Sie an der entsprechenden Stelle im URL <USER> (in Großbuchstaben) ein. Wenn Sie einen Namen und eine Beschreibung für das Lesezeichen angeben, werden diese Informationen anstelle des URLs auf der IVE-Startseite angezeigt.
  - 2 Damit die Webseite als erste Seite angezeigt wird, nachdem sich der Benutzer beim IVE angemeldet hat, klicken Sie nach **Start Page** auf **Yes**. Nachdem sich ein Benutzer angemeldet hat, wird diese Seite mit der IVE-Symboleiste zum Durchsuchen angezeigt, wodurch ein schneller Zugriff auf die IVE-Startseite ermöglicht wird.
  - 3 Klicken Sie auf **Save** oder **Save & Add Another**. Wenn Sie das Hinzufügen von Lesezeichen beendet haben, wählen Sie die Gruppenregisterkarte **Web > General** aus.

- 4
- Vergewissern Sie sich, dass für die Autorisierungsgruppe die entsprechenden Optionen für Webbrowsing konfiguriert wurden. Weitere Informationen finden Sie unter „Web > Unterregisterkarte „Access Control““ auf Seite 158.

**Hinweis:** Bei Lesezeichen für Webseiten, die clientseitige Java-Applets enthalten, müssen Sie die Unterstützung für clientseitige Java-Applets aktivieren.

**Zusätzliche Aufgaben**

- Klicken Sie zum Bearbeiten eines Lesezeichens auf dessen Namen, und führen Sie die Änderungen dann entsprechend den oben angegebenen Richtlinien durch.
- Um ein Lesezeichen zu löschen, aktivieren Sie das Kontrollkästchen neben dem jeweiligen Namen, und klicken Sie auf **Delete**.
- Klicken Sie zum Sortieren von Lesezeichen auf **Sort**, markieren Sie ein Lesezeichen, ändern Sie die Position über die Schaltfläche **Nach oben** oder **Nach unten**, und klicken Sie dann auf **Save Changes**.



**Abbildung 67: Authentication & Authorization > Authorization Groups > GroupName > Web > Bookmarks**

## Web > Unterregisterkarte „Java Socket ACL“

### ☒ **Angeben der Server, mit denen Java-Applets eine Verbindung herstellen können**

Auf dieser Registerkarte können Sie angeben, mit welchen Servern und Ports Java-Applets eine Verbindung herstellen können.

#### **So geben Sie an, mit welchen Servern Java-Applets eine Verbindung herstellen können**

1. Wählen Sie in der Administratorkonsole das Menü **Authentication & Authorization > Authorization Groups** und anschließend eine Gruppe aus.
2. Wählen Sie aus den Gruppenregisterkarten **Web > Java Socket ACL** aus.  
Benutzerdefinierte Autorisierungsgruppen erben standardmäßig die Einstellungen der Benutzergruppe. Klicken Sie zum Festlegen benutzerdefinierter Einstellungen auf **Use custom settings** und anschließend auf **Update**.
3. Geben Sie einen Servernamen ein. Sie können auch Ports angeben.
4. Klicken Sie auf **Save Changes**.

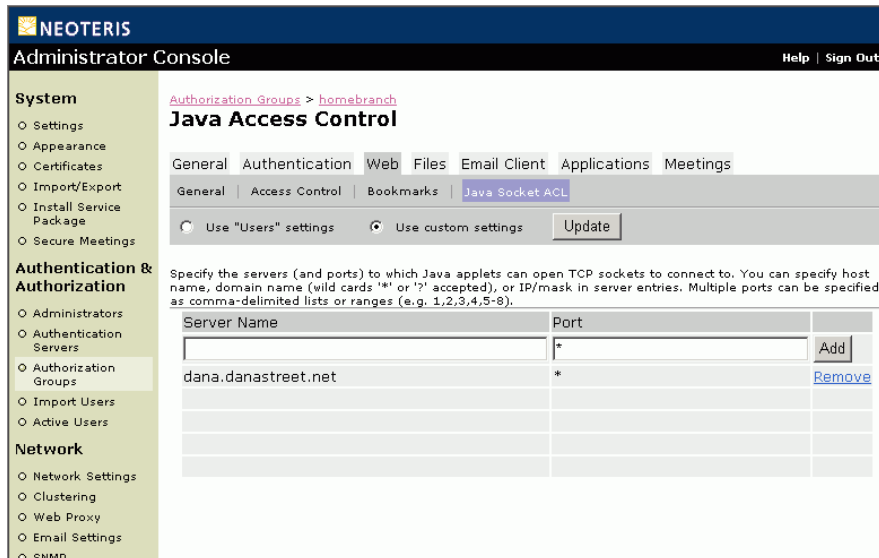


Abbildung 68: Authentication & Authorization > Authorization Groups > GroupName > Web > Java Socket ACL

## Files > Unterregisterkarte „General“

### ☑ Steuern des Netzwerkzugriffs unter Windows und UNIX/NFS

Auf dieser Registerkarte können Sie die Optionen der Benutzer zum Durchsuchen von Windows- und UNIX/NFS-Netzwerken angeben, einschließlich der Möglichkeit, Ressourcen anzuzeigen und Ordnerlesezeichen zu erstellen. Diese Optionen können zusammen mit der Zugriffssteuerungsrichtlinie von Windows (Seite 164) bzw. UNIX/NFS (Seite 172) verwendet werden.

#### So definieren Sie allgemeine Einstellungen für das Durchsuchen des Netzwerks

1. Wählen Sie in der Administratorkonsole das Menü **Authentication & Authorization > Authorization Groups** und anschließend eine Gruppe aus.
2. Wählen Sie aus den Gruppenregisterkarten **Files > General** aus.

3. Wählen Sie die Einstellungen für die jeweiligen Optionen aus, und klicken Sie anschließend auf **Save Changes**. Für Windows und UNIX/NFS stehen unter anderem folgende Optionen zur Verfügung:
  - **Users can view any allowed resources and add bookmarks**  
Diese Option ermöglicht es Benutzern, Lesezeichen für Ressourcen in verfügbaren Dateifreigaben anzuzeigen und zu erstellen.
  - **Users can view any allowed resources**  
Diese Option ermöglicht es Benutzern, zu Ressourcen in verfügbaren Dateifreigaben zu wechseln.
  - **Users can view bookmarked resources only**  
Diese Option ermöglicht es den Benutzern lediglich, zu administratordefinierten Lesezeichen für verfügbare Dateifreigaben zu wechseln.
  - **Windows networking disabled or UNIX/NFS Networking disabled**  
Bei dieser Option können die Benutzer zu keinerlei Dateiressourcen wechseln. Verwenden Sie diese Option, wenn Sie die Zugriffsmöglichkeiten schnell ändern müssen, die Richtlinien zum Durchsuchen von Dateien sowie Zugriffssteuerungslisten jedoch erhalten bleiben sollen. Wenn Sie diese Option auswählen, werden auf der IVE-Startseite keine Elemente der Benutzeroberfläche für den Netzwerkzugriff mehr angezeigt.

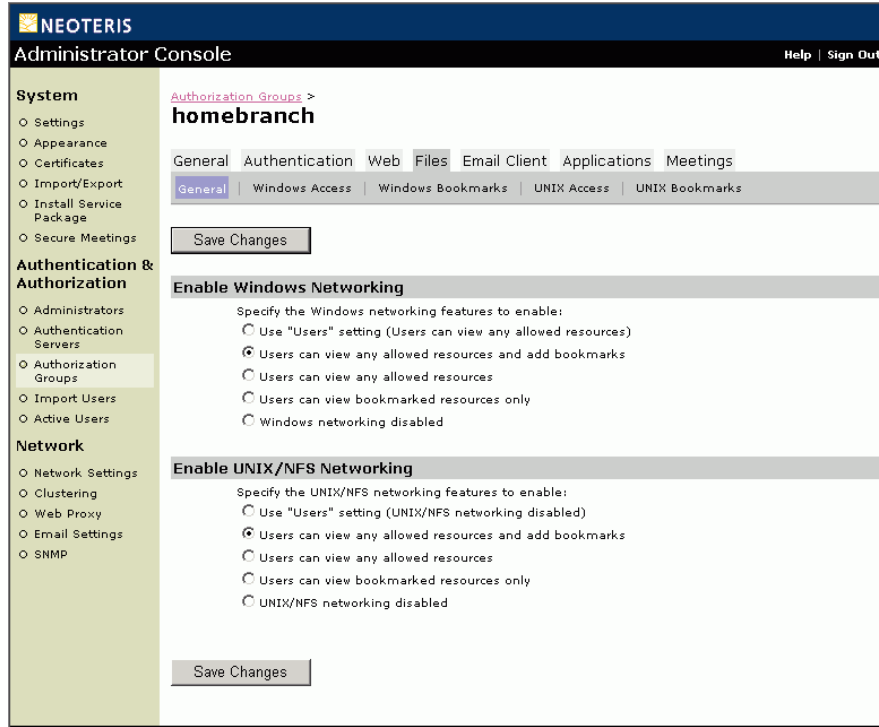


Abbildung 69: Authentication & Authorization > Authorization Groups > GroupName > Files > General

## Files > Unterregisterkarte „Windows Access“

### ☒ Zugriffssteuerung für Windows-Ressourcen


Wenn Sie über ein Windows-Netzwerk verfügen und die Windows-Ressourcen festlegen möchten, auf die Benutzer zugreifen können, können Sie zwischen den beiden folgenden Optionen auswählen:

- Eine **open policy** (Standard), mit der der Zugriff auf alle Windows-Ressourcen gewährt wird, mit Ausnahme derer in der Liste **Denied Resource**. Wenn Sie eine „open policy“ (offene Richtlinie) festlegen, wird den Benutzern eine gefilterte Netzwerkumgebung angezeigt.
- Eine **closed policy**, mit der der Zugriff auf alle Windows-Ressourcen verweigert wird, mit Ausnahme derer in der Liste **Allowed Resource**. Wenn Sie eine „closed policy“ (geschlossene Richtlinie) festlegen, wird den Benutzern eine Liste der Ordnerressourcen angezeigt, auf die zugegriffen werden kann.

Windows-Ressourcen werden zugelassen oder verweigert, indem Sie zum Server und der Freigabe wechseln oder diese eingeben und bei Bedarf zusätzlich den Pfad zu einem bestimmten Ordner angeben.

### So steuern Sie den Zugriff auf Windows-Ressourcen

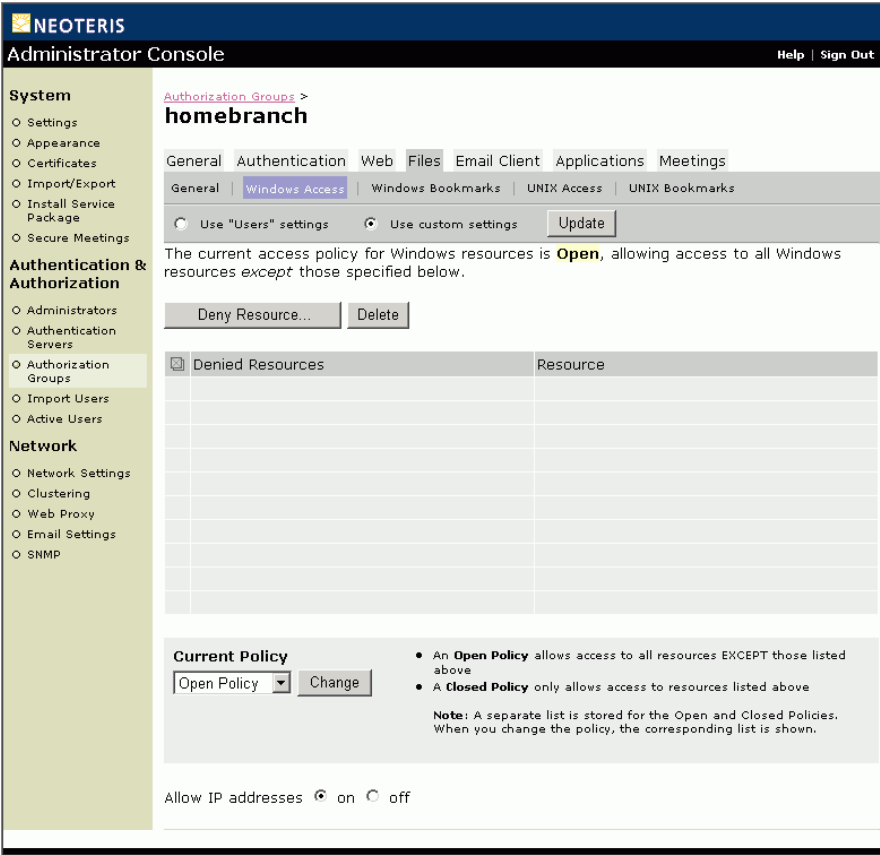
1. Wählen Sie in der Administratorkonsole das Menü **Authentication & Authorization > Authorization Groups** und anschließend eine Gruppe aus.
2. Wählen Sie aus den Gruppenregisterkarten **Files > Windows Access** aus. Benutzerdefinierte Autorisierungsgruppen erben standardmäßig die Einstellungen der Benutzergruppe. Klicken Sie zum Festlegen benutzerdefinierter Einstellungen auf **Use custom settings** und anschließend auf **Update**.
3. Geben Sie im Dropdownfeld **Current Policy** entweder eine geschlossene oder eine offene Richtlinie an, und klicken Sie auf **Change**.
4. Wenn Sie in Schritt 4 eine geschlossene Richtlinie ausgewählt haben, fahren Sie mit Schritt 7 fort. Wenn Sie eine offene Richtlinie ausgewählt haben, fügen Sie der Liste **Denied Resources** folgendermaßen Ressourcen hinzu, auf die Benutzer nicht zugreifen sollen:
  - 1 Klicken Sie auf **Deny Resource**.
  - 2 Geben Sie bei Bedarf einen Namen und eine Beschreibung für die Ressource an. Der angegebene Ressourcenname wird anstelle des UNC- oder URL-Namens in der Liste **Denied Resources** angezeigt.

- 3 Klicken Sie auf **Browse**, und navigieren Sie zum Server und der Freigabe, die verweigert werden sollen.  
Verwenden Sie NetBIOS-Namen, da die Angabe von Windows-Ressourcen nach IP-Adresse zu fehlerhaftem Verhalten führt.
- 4 Wenn es sich bei der Ressource, die verweigert werden soll, um einen Unterordner handelt, geben Sie den Pfad im Feld **Path** an.
- 5 Klicken Sie auf **Add Resource**. Benutzern wird die Ressource beim nächsten Zugriff auf die Seite **Windows Files** nicht mehr angezeigt.
5. Wenn Sie in Schritt 4 eine geschlossene Richtlinie ausgewählt haben, fügen Sie zur Liste **Allowed Resources** folgendermaßen Ressourcen hinzu, auf die die Benutzer zugreifen dürfen:
  - 1 Klicken Sie auf **Allow Resource**.
  - 2 Geben Sie bei Bedarf einen Namen und eine Beschreibung für die Ressource an. Der angegebene Ressourcenname wird IVE-Benutzern anstelle des Ressourcenspeicherortes angezeigt. Die eingegebene Beschreibung wird IVE-Benutzern ebenfalls angezeigt.
  - 3 Klicken Sie auf **Browse**, und navigieren Sie zum Server und der Freigabe, die zugelassen werden sollen.  
Verwenden Sie NetBIOS-Namen, da die Angabe von Windows-Ressourcen nach IP-Adresse zu fehlerhaftem Verhalten führt.
  - 4 Wenn es sich bei der Ressource, die zugelassen werden soll, um einen Unterordner handelt, geben Sie den Pfad im Feld **Path** an.
  - 5 Um die Ressource im schreibgeschützten Modus hinzuzufügen, wählen Sie **Read only** aus. Die Benutzer können in einer schreibgeschützten Ressource keine Ordner erstellen und keine Dateien hochladen.
  - 6 Damit die Benutzer die Unterverzeichnisse der Ressource anzeigen können, wählen Sie **Show subdirectories** aus.
  - 7 Um die Typen von Dateien einzuschränken, die den Benutzern angezeigt werden, wählen Sie **Show only files of a specific type** aus, und geben Sie die Dateierweiterung für jeden zugelassenen Dateityp ein.
  - 8 Klicken Sie auf **Add Resource**. Benutzern wird die hinzugefügte Ressource auf der Seite **Windows Files** angezeigt, wenn sie das nächste Mal auf die Seite zugreifen.
6. Wenn Sie eine geschlossene Richtlinie verwenden, werden die Benutzer standardmäßig aufgefordert, Anmeldeinformationen (Benutzername und Kennwort) für geschützte Ressourcen einzugeben. Stattdessen können Sie folgendermaßen einen Benutzernamen und ein Kennwort festlegen, das Gruppenmitglieder beim Zugriff auf eine Ressource verwenden sollten:
  - 1 Klicken Sie auf das  Symbol für die Ressource.
  - 2 Vervollständigen Sie die Seite „**Access With**“ **Account**.



- ### Zusätzliche Aufgaben:

- Um die Ressourceneinstellungen zu bearbeiten, klicken Sie auf die Ressourcenverknüpfung in der Ressourcenliste.
- Um eine Windows-Ressource zu löschen, aktivieren Sie das entsprechende Kontrollkästchen, und klicken Sie auf **Delete**.



**Abbildung 70: Authentication & Authorization > Authorization Groups > *GroupName* > Files > Windows Access**

## Files > Unterregisterkarte „Windows Bookmarks“

### ☒ Erstellen von Lesezeichen für Windows-Ressourcen

Auf dieser Registerkarte können Sie Windows-Lesezeichen erstellen, die auf der IVE-Startseite angezeigt werden. Sie können den IVE-Benutzernamen des Benutzers in den URL-Pfad einfügen, um so einen schnellen Zugriff auf die Netzwerkverzeichnisse des Benutzers zu ermöglichen.

#### So erstellen Sie ein Windows-Lesezeichen

1. Wählen Sie in der Administratorkonsole das Menü **Authentication & Authorization > Authorization Groups** und anschließend eine Gruppe aus.
2. Wählen Sie aus den Gruppenregisterkarten **Files > Windows Bookmarks** aus. Benutzerdefinierte Autorisierungsgruppen erben standardmäßig die Einstellungen der Benutzergruppe. Klicken Sie zum Festlegen benutzerdefinierter Einstellungen auf **Use custom settings** und anschließend auf **Update**.
3. Klicken Sie zum Erstellen des Lesezeichens auf **New**:
4. Geben Sie die Einstellungen für das Lesezeichen an:
  - 1 Wechseln Sie zum Server und Sharenamen, bzw. geben Sie diesen ein. Geben Sie einen Pfad ein, um den Zugriff weiter einzuschränken. Wenn Sie den Benutzernamen des Benutzers einfügen möchten, geben Sie an der entsprechenden Stelle im Pfad <USER> (in Großbuchstaben) ein. Wenn Sie einen Namen und eine Beschreibung für das Lesezeichen angeben, werden diese Informationen anstelle des Servers/der Freigabe auf der IVE-Startseite angezeigt.
  - 2 Klicken Sie auf **Add Resource**. Wenn Sie das Hinzufügen von Lesezeichen beendet haben, wählen Sie die Gruppenregisterkarte **Files > General** aus.
  - 3 Vergewissern Sie sich, dass die entsprechenden Windows-Netzwerkoptionen für die Autorisierungsgruppe konfiguriert wurden. Weitere Informationen finden Sie unter „Files > Unterregisterkarte „General““ auf Seite 164.

---

**Hinweis:** Ein Windows-Server kann nicht mit einem Lesezeichen versehen werden. Sie müssen sowohl den Server- als auch den Freigabenamen angeben.

---

Zusätzliche Aufgaben

- Klicken Sie zum Bearbeiten eines Lesezeichens auf dessen Namen, und führen Sie die Änderungen dann entsprechend den oben angegebenen Richtlinien durch.
- Um ein Lesezeichen zu löschen, aktivieren Sie das Kontrollkästchen neben dem jeweiligen Namen, und klicken Sie auf **Delete**.
- Klicken Sie zum Sortieren von Lesezeichen auf **Sort**, markieren Sie ein Lesezeichen, ändern Sie die Position über die Schaltfläche **Nach oben** oder **Nach unten**, und klicken Sie dann auf **Save Changes**.

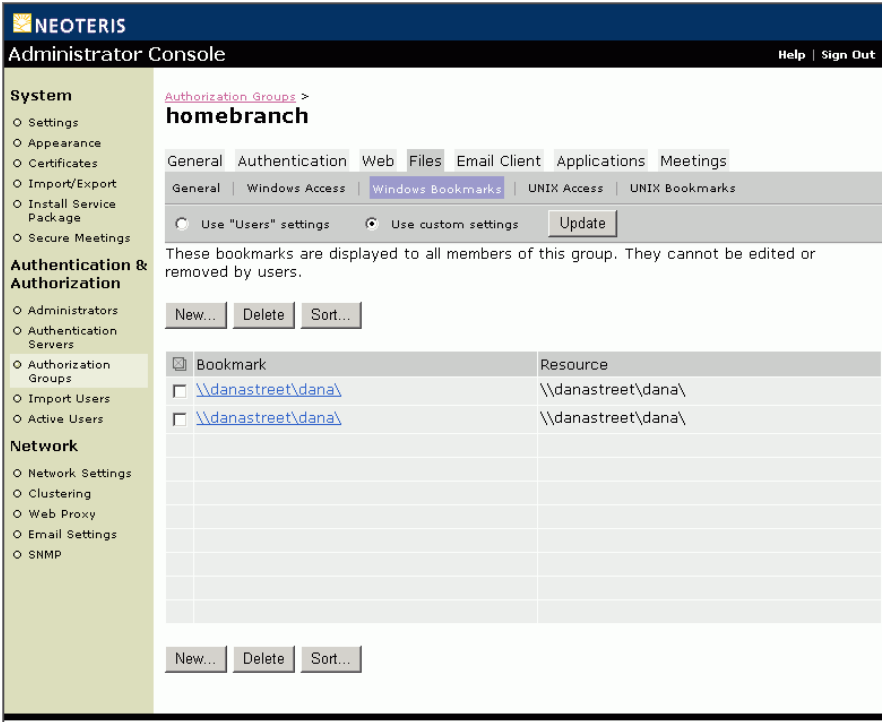


Abbildung 71: Authentication & Authorization > Authorization Groups > GroupName > Files > Windows Bookmarks

## Files > Unterregisterkarte „UNIX Access“

### ☒ Zugriffssteuerung für UNIX/NFS-Ressourcen

Wenn UNIX/NFS-Ressourcen für Benutzer zugänglich sein sollen, müssen Sie angeben, auf welche Ressourcen über die Seite **Access Control > UNIX/NFS** zugegriffen werden kann. UNIX/NFS-Ressourcen werden zugelassen, indem Sie den Serverhostnamen oder die IP-Adresse eingeben und den Pfad zu einer bestimmten Freigabe angeben.

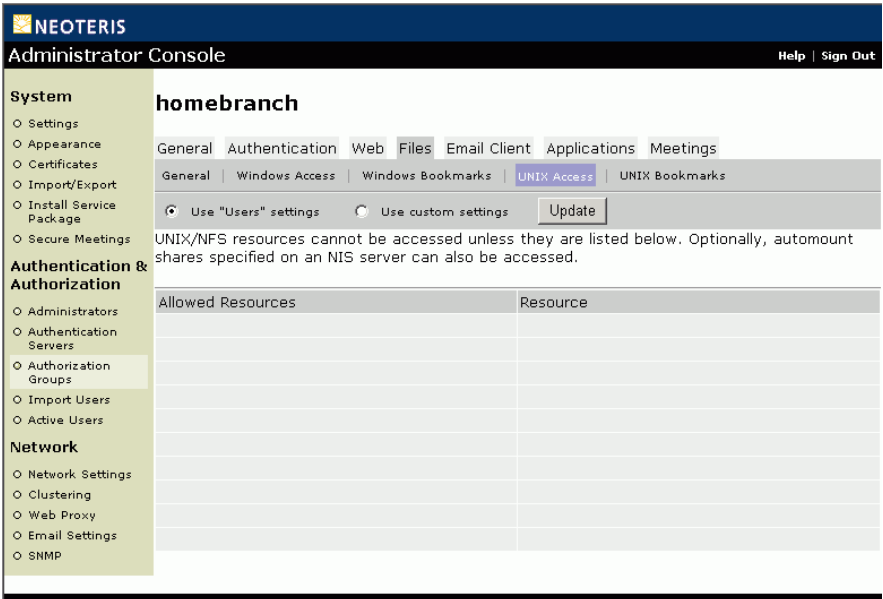
#### So steuern Sie den Zugriff auf UNIX/NFS-Ressourcen

1. Wählen Sie in der Administratorkonsole das Menü **Authentication & Authorization > Authorization Groups** und anschließend eine Gruppe aus.
2. Wählen Sie aus den Gruppenregisterkarten **Files > UNIX Access** aus.  
Benutzerdefinierte Autorisierungsgruppen erben standardmäßig die Einstellungen der Benutzergruppe. Klicken Sie zum Festlegen benutzerdefinierter Einstellungen auf **Use custom settings** und anschließend auf **Update**.
3. Klicken Sie auf **Allow Resource**, und vervollständigen Sie die Seite **Allow UNIX/NFS Resource** folgendermaßen:
  - 1 Geben Sie bei Bedarf einen Namen und eine Beschreibung für die Ressource an. Der angegebene Ressourcename wird IVE-Benutzern anstelle des Ressourcenspeicherortes angezeigt. Die eingegebene Beschreibung wird IVE-Benutzern ebenfalls angezeigt.
  - 2 Geben Sie den Hostnamen oder die IP-Adresse des Servers ein, und geben Sie den Pfad zu einer bestimmten Freigabe ein, die zugelassen werden soll.
  - 3 Um die Ressource im schreibgeschützten Modus hinzuzufügen, wählen Sie **Read only** aus. Die Benutzer können in einer schreibgeschützten Ressource keine Ordner erstellen und keine Dateien hochladen.
  - 4 Damit die Benutzer die Unterverzeichnisse der Ressource anzeigen können, wählen Sie **Show subdirectories** aus.
  - 5 Um die Typen von Dateien einzuschränken, die den Benutzern angezeigt werden, wählen Sie **Show only files of a specific type** aus, und geben Sie die Dateierweiterung für jeden zugelassenen Dateityp ein.
  - 6 Klicken Sie auf **Add Resource**. Benutzern wird die hinzugefügte Ressource auf der Seite **UNIX/NFS Files** angezeigt, wenn sie das nächste Mal auf die Seite zugreifen.

4. Um Automount-Freigaben von NIS zuzulassen, wählen Sie **Allow the resources...** aus, und geben Sie den Hostnamen oder die IP-Adresse des NSI-Servers sowie die NIS-Domäne an.
5. Klicken Sie auf **Save Changes**.

**Zusätzliche Aufgaben:**

- Um die Ressourceneinstellungen zu bearbeiten, klicken Sie auf die Ressourcenverknüpfung in der Ressourcenliste.
- Um eine UNIX/NFS-Ressource zu löschen, aktivieren Sie das entsprechende Kontrollkästchen, und klicken Sie auf **Delete**.



**Abbildung 72:** Authentication & Authorization > Authorization Groups > GroupName > Files > UNIX Access

## Files > Unterregisterkarte „UNIX Bookmarks“

### ☒ Erstellen von Lesezeichen für UNIX-Ressourcen

Auf dieser Registerkarte können Sie UNIX/NFS-Lesezeichen erstellen, die auf der IVE-Startseite angezeigt werden. Sie können den IVE-Benutzernamen des Benutzers in den URL-Pfad einfügen, um so einen schnellen Zugriff auf die Netzwerkverzeichnisse des Benutzers zu ermöglichen.

#### So erstellen Sie ein UNIX/NFS-Lesezeichen

1. Wählen Sie in der Administratorkonsole das Menü **Authentication & Authorization > Authorization Groups** und anschließend eine Gruppe aus.
2. Wählen Sie aus den Gruppenregisterkarten **Files > UNIX Bookmarks** aus.  
Benutzerdefinierte Autorisierungsgruppen erben standardmäßig die Einstellungen der Benutzergruppe. Klicken Sie zum Festlegen benutzerdefinierter Einstellungen auf **Use custom settings** und anschließend auf **Update**.
3. Klicken Sie zum Erstellen des Lesezeichens auf **New**:
4. Geben Sie die Einstellungen für das Lesezeichen an:
  - 1 Geben Sie den Hostnamen oder die IP-Adresse des Servers und den Pfad zu der Freigabe ein. Wenn Sie den Benutzernamen des Benutzers einfügen möchten, geben Sie an der entsprechenden Stelle im Pfad <USER> (in Großbuchstaben) ein. Wenn Sie einen Namen und eine Beschreibung für das Lesezeichen angeben, werden diese Informationen anstelle des Servers/Pfades auf der IVE-Startseite angezeigt.
  - 2 Klicken Sie auf **Add Resource**. Wenn Sie das Hinzufügen von Lesezeichen beendet haben, wählen Sie die Gruppenregisterkarte **Files > General** aus.
  - 3 Vergewissern Sie sich, dass die entsprechenden Windows-Netzwerkoptionen für die Autorisierungsgruppe konfiguriert wurden. Weitere Informationen finden Sie unter „Files > Unterregisterkarte „General““ auf Seite 164.

Zusätzliche Aufgaben

- Klicken Sie zum Bearbeiten eines Lesezeichens auf dessen Namen, und führen Sie die Änderungen dann entsprechend den oben angegebenen Richtlinien durch.
- Um ein Lesezeichen zu löschen, aktivieren Sie das Kontrollkästchen neben dem jeweiligen Namen, und klicken Sie auf **Delete**.
- Klicken Sie zum Sortieren von Lesezeichen auf **Sort**, markieren Sie ein Lesezeichen, ändern Sie die Position über die Schaltfläche **Nach oben** oder **Nach unten**, und klicken Sie dann auf **Save Changes**.

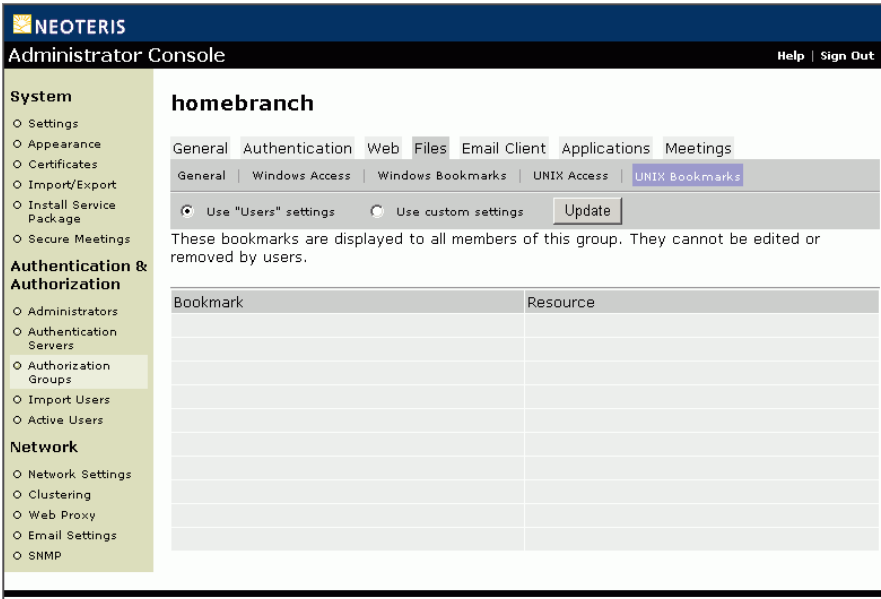


Abbildung 73: Authentication & Authorization > Authorization Groups > GroupName > Files > UNIX Bookmarks

## Registerkarte „Email Client“

### ☒ Aktivieren der Aktualisierungsoption für den Secure Email Client

Welche E-Mail-Unterstützung vom IVE gewährt wird, hängt von den optionalen Funktionen ab, die für den IVE-Server lizenziert sind:

- **Aktualisierungsoption für den Secure Email Client**

Wenn Ihre IVE-Lizenz die Aktualisierungsoption für den Secure Email Client umfasst, unterstützt das IVE IMAP4 (Internet Mail Application Protocol), POP3 (Post Office Protocol) und SMTP (Simple Mail Transfer Protocol). Sie können den Zugriff auf die IMAP/POP/SMTP-Mailserver der Firma ganz einfach aktivieren, indem Sie den Mailserver, die E-Mail-Sitzung und die Authentifizierungsinformationen auf der Seite **Network > Email Settings** angeben (Seite 267). Auf dieser Seite werden die Standardeinstellungen für alle Gruppen bestimmt. Auf der Registerkarte **Messaging > General** können Sie die Option für den Secure Email Client gruppenweise aktivieren oder deaktivieren.

---

**Wichtig:** Wenn Sie das IVE auf der Seite **Network > Email Settings** nicht als E-Mail-Proxy zulassen, kann die Option für den Secure Email Client von keiner Gruppe verwendet werden.

---

- **Aktualisierungsoption für Secure Application Manager**

Wenn Ihre IVE-Lizenz die Aktualisierungsoption für Secure Application Manager umfasst, unterstützt das IVE das systemeigene MAPI-Protokoll von Microsoft Exchange und das systemeigene Lotus Notes-Protokoll. Sie können den Zugriff auf Microsoft Exchange Server und Lotus Notes Server auf der Registerkarte **Applications** einer Autorisierungsgruppe aktivieren.



## So ermöglichen Sie einer Autorisierungsgruppe die Verwendung des Secure Email Client

1. Wählen Sie in der Administratorkonsole das Menü **Authentication & Authorization > Authorization Groups** und anschließend eine Gruppe aus.
2. Wählen Sie aus den Gruppenregisterkarten **Email Client** aus.
3. Wählen Sie die entsprechende Option aus, und klicken Sie dann auf **Save Changes**. Folgende Optionen stehen zur Verfügung:
  - **Use Users group settings**  
Wendet die Einstellungen der Benutzergruppe an.
  - **Enabled**  
Ermöglicht es der Gruppe, die auf der Seite **Network > Email Settings** festgelegten Einstellungen zu verwenden. Sie müssen das IVE auf dieser Seite als E-Mail-Proxy aktivieren, damit die Gruppe diese Einstellungen verwenden kann.
  - **Disabled**  
Verweigert der Gruppe die Verwendung der Aktualisierungsoption für den Secure Email Client.

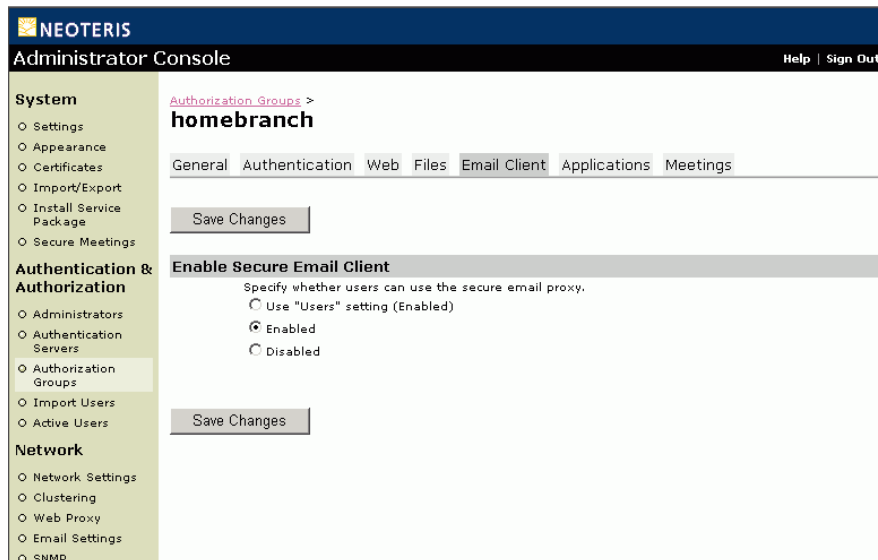


Abbildung 74: Authentication & Authorization > Authorization Groups > GroupName > Email Client

## Applications > Unterregisterkarte „General“

### ☒ Angeben von allgemeinen Client-/Server-Anwendungseinstellungen

Verwenden Sie die Unterregisterkarte **Applications > General** zum Aktivieren der folgenden Optionen:

- **Aktualisierungsoption für den sicheren Terminalzugriff**

Gewährt Zugriff auf eine Reihe von Netzwerkgeräten, beispielsweise UNIX-Server, im Netzwerk betriebene Geräte und Legacyanwendungen, die das Terminal verwenden.

- **Aktualisierungsoption für Secure Application Manager**

Vermittelt die Remotekommunikation mit internen Client/Server-Anwendungen über SSL, mit Optionen für Implementierungen unter Windows oder Java.

Eine Übersicht über

- W-SAM finden Sie unter „Applications > Unterregisterkarte „Secure Application Manager (W-SAM)““ auf Seite 187.
- J-SAM finden Sie unter „Applications > Unterregisterkarte „Secure Application Manager (J-SAM)““ auf Seite 193.

---

**Wichtig:** Auf der Unterregisterkarte **Applications > General** werden Konfigurationsoptionen angezeigt, die der aktivierten Version von Secure Application Manager entsprechen. **Abbildung 77** auf Seite 191 zeigt die Unterregisterkarte „General“, wenn W-SAM aktiviert ist. **Abbildung 80** auf Seite 200 zeigt die Unterregisterkarte „General“, wenn J-SAM aktiviert ist.

---

### So geben Sie allgemeine Client-/Server-Anwendungseinstellungen an

1. Wählen Sie in der Administratorkonsole das Menü **Authentication & Authorization > Authorization Groups** und anschließend eine Gruppe aus.
2. Wählen Sie aus den Gruppenregisterkarten **Applications > General** aus.

3. Wählen Sie eine der folgenden Optionen aus, und klicken Sie dann auf **Save Changes**. Folgende Optionen stehen zur Verfügung:

- **Enable Secure Terminal Access**

Wenn der IVE-Server mit der optionalen Aktualisierungsoption für sicheren Terminalzugriff lizenziert ist, können Sie den Telnet- oder SSH-Zugriff auf Firmenressourcen über einen Webbrowser ermöglichen. Folgende Optionen stehen zur Verfügung:

- **User „Users“ setting**

Wendet die Einstellungen der Benutzergruppe an.

- **Enabled and users can add bookmarks**

Ermöglicht es einer Gruppe, die von Ihnen definierten Lesezeichen für den Terminalzugriff zu verwenden und ihre eigenen Lesezeichen zu definieren. Wenn Sie diese Option aktivieren, wird auf der Seite **Terminal Sessions** die Schaltfläche **Add Terminal Session** angezeigt, wenn ein Benutzer die IVE-Startseite das nächste Mal aktualisiert.

- **Enabled**

Ermöglicht es einer Gruppe, die von Ihnen definierten Lesezeichen für den Terminalzugriff auszuführen.

- **Disabled**

Deaktiviert die Option für den sicheren Terminalzugriff.

Informationen zum Erstellen von Lesezeichen finden Sie unter „Erstellen von Lesezeichen für sichere Terminalsitzungen“ auf Seite 185.

- **Enable Secure Application Manager**

Wenn der IVE-Server mit der optionalen Aktualisierungsoption für Secure Application Manager lizenziert ist, können Sie Benutzern den Zugriff auf Client-/Server-Anwendungen über einen Webbrowser ermöglichen. Folgende Optionen stehen zur Verfügung:

- **User „Users“ setting**

Wendet die Einstellungen der Benutzergruppe an.

- **Enabled using the Windows version (Access Control)**

Aktiviert die Windows-Version von Secure Application Manager. Weitere Informationen zu W-SAM finden Sie unter „Applications > Unterregisterkarte „Secure Application Manager (W-SAM)““ auf Seite 187.

- **Enabled using the Windows version with Netbios support (Access Control).**

Aktiviert die Windows-Dateifreigabe unter Verwendung des NetBIOS-Protokolls für Nachrichtenverkehr im Zusammenhang mit Dateioperationen. Diese Option bietet Benutzern die Möglichkeit, auf dem Remotenetzwerk Laufwerke zuzuordnen, auf freigegebene Firmendateien zuzugreifen und Dateien mit Windows Explorer zu öffnen.

Weitere Informationen zu W-SAM finden Sie unter „Applications > Unterregisterkarte „Secure Application Manager (W-SAM)““ auf Seite 187.

---

**Wichtig:** Wenn Sie diese Option aktivieren, müssen Sie auch die W-SAM-Zugriffssteuerungsliste konfigurieren, die angibt, an welche Unternehmensressourcen (auf der Grundlage der IP-Adresse/Port-Kombination) die Anforderung einer Anwendung oder eines Hosts gesendet werden kann. Um diese Liste anzugeben, klicken Sie in dieser Option auf die Verknüpfung **Access Control**. Sie müssen außerdem Anwendungen und Hosts festlegen, die mit W-SAM gesichert werden sollen. Weitere Informationen erhalten Sie unter „Festlegen von Anwendungen und Hosts, die mit W-SAM gesichert werden sollen.“ auf Seite 189.

---

- **Enabled using the Java Session Manager and users can add applications**

Aktiviert die Java-Version von Secure Application Manager, und ermöglicht es den Benutzern, Anwendungen hinzuzufügen. Damit Benutzer Anwendungen hinzufügen können, müssen Sie den DNS-Namen und die Client/Serverports des Anwendungsservers kennen.

Wenn Sie diese Option aktivieren, können Benutzer die Portumleitung zu einem beliebigen Host oder Port im Unternehmen einrichten. Bevor Sie Benutzern die Möglichkeit geben, Anwendungen hinzuzufügen, vergewissern Sie sich, dass diese Funktion mit Ihren Sicherheitsanforderungen vereinbar ist. Wenn ein Benutzer eine Anwendung hinzufügt, bleibt diese Anwendung für den Benutzer auch dann verfügbar, wenn Sie die Einstellung später in **Enabled** ändern, oder wenn Sie diese Funktion deaktivieren und später wieder aktivieren.

- **Enabled using the Java Session Manager**

Aktiviert die Java-Version von Secure Application Manager und ermöglicht es Benutzern, die von Ihnen installierten Anwendungen auszuführen.

- **Enable Automatic Launch of the Secure Application Manager**

Startet Secure Application Manager, wenn sich ein Benutzer anmeldet. Wenn Sie nicht **Yes** auswählen, müssen die Benutzer Secure Application Manager manuell über das Menü **Client Applications** starten.

## Zusätzliche Optionen bei aktiviertem J-SAM

Wenn Sie die Java-Version von Secure Application Manager aktivieren, werden auf der Unterregisterkarte **Applications > General** zusätzliche Konfigurationsoptionen angezeigt, die unten beschrieben werden. Beachten Sie, dass die Clientanwendung eine Verbindung mit dem lokalen Computer herstellen muss, auf dem Secure Application Manager als Anwendungsserver ausgeführt wird, damit die Java-Version von Secure Application Manager fehlerfrei verwendet werden kann. Die empfohlene Vorgehensweise für das Zuordnen von Anwendungsservern zum lokalen PC eines Benutzers besteht in der Aktivierung der automatischen Hostzuordnung, wodurch das IVE die Datei `hosts` automatisch so ändern kann, dass Anwendungsserver zum lokalen Host für sichere Portumleitung geleitet werden.

---

**Wichtig:** Die automatische Hostzuordnung kann auf Windows-PCs nur erfolgen, wenn die Benutzer über Administratorrechte verfügen und Secure Application Manager daher die Datei `hosts` ändern kann. Wenn Benutzer nicht über Administratorrechte verfügen, wird im Secure Application Manager-Fenster eine Fehlermeldung angezeigt, und die Benutzer können nicht auf Client/Serveranwendungen zugreifen. Wenn die Sicherheitsrichtlinie das Erteilen von Administratorrechten an Benutzer nicht zulässt, können Sie die externen DNS-Server auch wie unter „Konfigurieren der externen DNS-Server und Benutzercomputer (falls erforderlich)“ auf Seite 201 beschrieben konfigurieren.

---

- **Enable Microsoft Exchange**

Wenn Sie die Java-Version von Secure Application Manager aktiviert haben, unterstützt das IVE das Microsoft Exchange MAPI-Protokoll (Messaging Application Programming Interface). Remotebenutzer können den Microsoft Outlook-Client auf ihren PCs zum Zugreifen auf E-Mail, ihre Kalender und andere Outlook-Funktionen über das IVE verwenden. Dafür müssen keine Änderungen am Outlook-Client vorgenommen werden, und es ist keine Verbindung auf Netzwerkebene, wie z. B. ein VPN, erforderlich. Die **Microsoft Exchange**-Verknüpfung wird auf der Seite **Client Applications** angezeigt, wenn sich ein Benutzer das nächste Mal beim IVE anmeldet.

Diese Funktion wird auf PCs unter Windows 2000 mit Internet Explorer 5.5 oder 6.0 und der Microsoft JVM unterstützt. Diese Funktion ist mit PCs unter Windows 98 (Internet Explorer 5.5) oder Windows XP (Internet Explorer 6.0) und der Microsoft JVM kompatibel.

- **User „Users“ setting**  
Wendet die Einstellungen der Benutzergruppe an.
- **Enabled with access control (Specify allowed MS Exchange Servers)**  
Ermöglicht den Zugriff auf die angegebenen Microsoft Exchange-Server von einem Microsoft Outlook-E-Mail-Client. Sie müssen diese Server auf der Unterregisterkarte **Applications > MS Exchange** konfigurieren. Sie können auf diese Unterregisterkarte auch zugreifen, indem Sie in dieser Option auf die Verknüpfung **MS Exchange** klicken. Weitere Informationen zum Erstellen der Zugriffssteuerungsliste finden Sie unter „Angaben zulässiger MS Exchange-Server“ auf Seite 207.
- **Enabled**  
Ermöglicht den Zugriff auf alle Microsoft Exchange-Server.
- **Disabled**  
Deaktiviert diese Option.
- **Enable Lotus Notes**  
Wenn der IVE-Server mit dem optionalen Secure Messaging lizenziert ist, unterstützt das IVE das Lotus Notes-Protokoll. Remotebenutzer können Lotus Notes auf ihrem PC verwenden, um über das IVE auf E-Mail, Kalender und weitere Lotus Notes-Anwendungen zuzugreifen. Dafür ist keine Verbindung auf Netzwerkebene, wie z. B. ein VPN, erforderlich. Secure Messaging wird auf PCs unter Windows 2000 mit Internet Explorer 5.5 oder 6.0 und der Microsoft JVM unterstützt.
- **User „Users“ setting**  
Wendet die Einstellungen der Benutzergruppe an.
- **Enabled with access control (Specify allowed Lotus Notes Servers)**  
Ermöglicht den Zugriff auf die angegebenen Lotus Notes-Server. Sie müssen diese Server auf der Unterregisterkarte **Applications > Lotus Notes** konfigurieren. Sie können auf diese Unterregisterkarte auch zugreifen, indem Sie in dieser Option auf die Verknüpfung **Lotus Notes** klicken. Weitere Informationen zum Erstellen der Zugriffssteuerungsliste finden Sie unter „Angaben zulässiger MS Exchange-Server“ auf Seite 207.
- **Enabled**  
Aktiviert den Zugriff auf alle Lotus Notes-Server.
- **Disabled**  
Deaktiviert diese Option.

- **Enable Citrix NFuse Integration**

- **User „Users“ setting**

- Wendet die Einstellungen der Benutzergruppe an.

- **Enabled (Configure Citrix NFuse parameters)**

- Aktiviert die Integration von Citrix NFuse. Die Citrix NFuse-Parameter können auf der Unterregisterkarte **Applications > Citrix NFuse** konfiguriert werden. Auf diese Unterregisterkarte können Sie in dieser Option auch über die Verknüpfung **Citrix NFuse** zugreifen.

- **Enabled**

- Aktiviert den Zugriff auf alle Lotus Notes-Server.

- **Disabled**

- Deaktiviert diese Option.

- **Enable Automatic Host Mapping (Java version only)**

Die Java-Version von Secure Application Manager kann nur dann verwendet werden, wenn zwischen der Clientanwendung und dem lokalen PC, auf dem Secure Application Manager als Anwendungsserver ausgeführt wird, eine Verbindung eingerichtet wird. Die empfohlene Vorgehensweise für das Zuordnen von Anwendungsservern zum lokalen PC eines Benutzers besteht in der Aktivierung der automatischen Hostzuordnung, wodurch das IVE die Datei hosts automatisch so ändern kann, dass Anwendungsserver für sichere Portumleitung zum lokalen Host des PCs geleitet werden. Sie können auch den externen DNS-Server konfigurieren. Weitere Informationen erhalten Sie unter „Konfigurieren der externen DNS-Server und Benutzercomputer (falls erforderlich)“ auf Seite 201.

- **User „Users“ setting**

- Wendet die Einstellungen der Benutzergruppe an.

- **Enabled (automatically edit local hosts file)**

- Secure Application Manager bearbeitet die Datei hosts des Windows-PCs und ersetzt Einträge von Windows-Anwendungsservern durch localhost. Diese Einträge werden auf die Originaldaten zurückgesetzt, wenn ein Benutzer Secure Application Manager schließt.

- **Disabled**

- Secure Application Manager kann die Datei hosts des Windows-PCs nicht bearbeiten und die Einträge von Windows-Anwendungsservern nicht durch localhost ersetzen. Sie müssen stattdessen den externen DNS-Server so konfigurieren, dass die Anwendungsserver dem lokalen PC eines Benutzers zugeordnet werden.

- **Enable Automatic Host Mapping for MS Exchange Servers (Java Version Only)**

Der PC eines Remotebenutzers muss MS Exchange-Server in die Adresse 127.0.01 auflösen. Wenn Sie die automatische Hostzuordnung für MS Exchange Server nicht aktivieren möchten, müssen Sie den externen DNS-Server so konfigurieren, dass MS Exchange-Servernamen in die PC-Adresse eines Benutzers aufgelöst werden, und den PC konfigurieren.

Die Java-Version von Secure Application Manager kann nur dann verwendet werden, wenn zwischen der Clientanwendung und dem lokalen PC, auf dem Secure Application Manager als Anwendungsserver ausgeführt wird, eine Verbindung eingerichtet wird. Die empfohlene Vorgehensweise für das Zuordnen von Anwendungsservern zum lokalen PC eines Benutzers besteht in der Aktivierung der automatischen Hostzuordnung, wodurch das IVE die Datei hosts automatisch so ändern kann, dass Anwendungsserver für sichere Portumleitung zum lokalen Host des PCs geleitet werden. Sie können auch den externen DNS-Server konfigurieren. Weitere Informationen erhalten Sie unter „Konfigurieren der externen DNS-Server und Benutzercomputer (falls erforderlich)“ auf Seite 201.

Sie können das IVE so konfigurieren, dass Exchange-Server automatisch der lokalen Arbeitsstation eines Benutzers zugeordnet werden, um eine sichere Portweiterleitung während der Secure Application Manager-Sitzung des Benutzers zu gewährleisten. Das einmalige Setup ist die einzige IVE-Konfiguration, die zur Verwendung der automatischen Hostzuordnung für den sicheren Nachrichtenaustausch mit Exchange Server erforderlich ist. Sie können auch den externen DNS-Server und die Einstellungen des Benutzers-PCs konfigurieren. Weitere Informationen erhalten Sie unter „Konfigurieren der externen DNS-Server und Benutzercomputer (falls erforderlich)“ auf Seite 201.

Wenn Sie beabsichtigen, J-SAM mit Microsoft Outlook zu verwenden, empfiehlt sich die Aktivierung der automatischen Hostzuordnung für MS Exchange Server.

- **User „Users“ setting**

Wendet die Einstellungen der Benutzergruppe an.

- **Enabled (automatically edit local hosts file)**

Wendet die Einstellungen der Benutzergruppe an.

- **Disabled**

Deaktiviert diese Option.



## Applications > Unterregisterkarte „Terminal Sessions“

### ☒ Erstellen von Lesezeichen für sichere Terminalsitzungen

Auf dieser Registerkarte legen Sie Informationen zu Terminalsitzungen für Telnet- oder SSH-Sitzungen fest, die Benutzer möglicherweise starten. Wenn Sie die Aktualisierungsoption für den sicheren Terminalzugriff aktivieren (siehe Seite 179), den Benutzern jedoch nicht die Möglichkeit bieten, eigene Lesezeichen zu erstellen, müssen Sie unbedingt die Lesezeichen der Terminalsitzungen für sie konfigurieren. Andernfalls können Benutzer diese Funktion nicht nutzen.

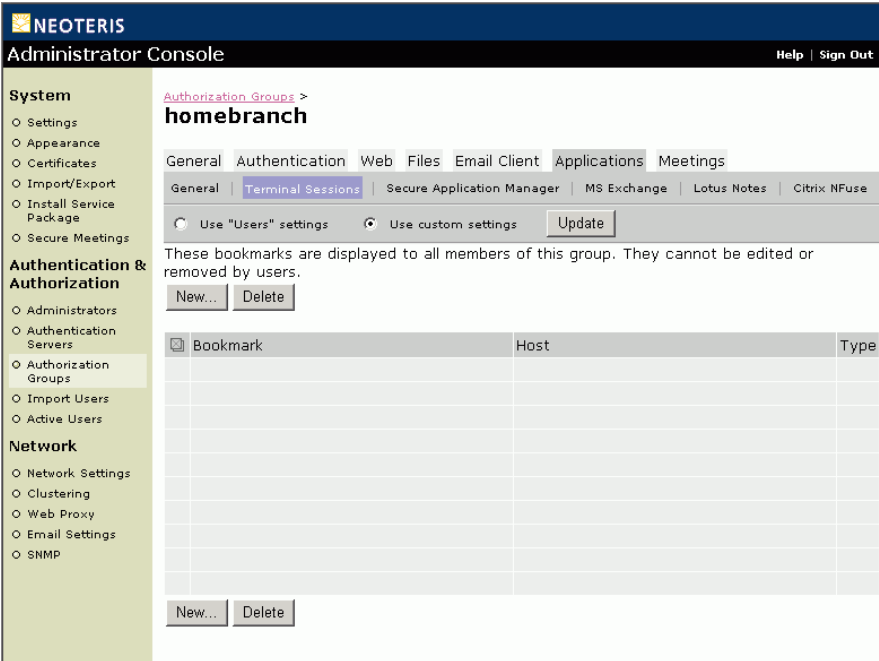
---

**Hinweis:** Gegenwärtig wird die Sun JVM in der Version 1.4.1 oder höher unterstützt.

---

### So erstellen Sie Lesezeichen für sichere Terminalsitzungen

1. Wählen Sie in der Administratorkonsole das Menü **Authentication & Authorization > Authorization Groups** und anschließend eine Gruppe aus.
2. Wählen Sie aus den Gruppenregisterkarten **Applications > General** aus.
3. Stellen Sie unter **Enable Secure Terminal Access** sicher, dass eine der **Enabled**-Optionen ausgewählt ist.
4. Wählen Sie aus den Gruppenregisterkarten **Applications > Terminal Sessions** aus.
5. Klicken Sie auf **New**, und geben Sie die erforderlichen Informationen ein, die durch ein Sternchen gekennzeichnet sind. Wenn Sie einen Namen und eine Beschreibung für ein Lesezeichen angeben, werden diese Informationen auf der Seite **Terminal Sessions** angezeigt.
6. Klicken Sie auf **Add Bookmark**, um das Lesezeichen auf der Seite **Terminal Sessions** hinzuzufügen.



**Abbildung 75:** Authentication & Authorization > Authorization Groups > *GroupName* > Applications > Terminal Sessions

## Applications > Unterregisterkarte „Secure Application Manager (W-SAM)“

Die Secure Application Manager-Aktualisierungsoption stellt sicheren Remotezugriff auf Anwendungsebene von Clientanwendungen auf Unternehmensserver bereit. Sie können zwei Versionen von Secure Application Manager bereitstellen:

- **Windows-Version (W-SAM)**

Die Windows-Version von Secure Application Manager ist eine Windows-32-Lösung für sicheres, transparentes Umleiten von ausgehenden TCP-Verbindungen über ein IVE-Gerät für jeweils eine Anwendung oder einen Host. Die Software wird von einem im IVE gehosteten ActiveX-Steuerelement heruntergeladen und gestartet.

- **Java-Version (J-SAM)**

Die Java-Version von Secure Application Manager bietet Unterstützung für statische TCP-Port-Client/Server-Anwendungen, darunter erweiterte Unterstützung für Microsoft MAPI, Lotus Notes und Citrix NFuse. Diese Version funktioniert in vielen Netzwerkkonfigurationen einwandfrei, unterstützt jedoch keine Client/Server-Anwendungen auf dynamischer TCP-Port-Basis.

Weitere Informationen zu J-SAM finden Sie unter „Applications > Unterregisterkarte „Secure Application Manager (J-SAM)““ auf Seite 193.

## Übersicht über Windows Secure Application Manager (W-SAM)

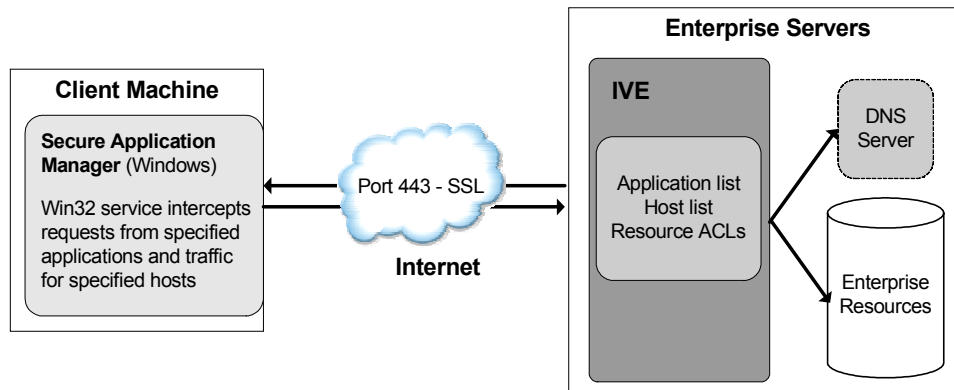
Die Windows-Version von Secure Application Manager (W-SAM) ist ein Dienst, der den LSP-Mechanismus (Layered Service Provider) verwendet, um Datenverkehr zu sichern, der von auf einem PC ausgeführten Client-Anwendungen stammt. Die LSP-Dienstkomponenten werden auf einem Client-PC unter Verwendung eines ActiveX-Steuerelements installiert, das heruntergeladen wird, wenn ein Benutzer Secure Application Manager von der IVE-Homepage aus startet. Sobald der Secure Application Manager installiert ist, fängt er folgende Anforderungen ab:

- TCP-Verbindungsaufrufe von im IVE konfigurierten Anwendungen
- DNS-Abfragen für im IVE konfigurierten Zielhostnamen

Wenn ein Benutzer Secure Application Manager startet<sup>1</sup>, wird ein Statusfenster als Prozess im System Tray ausgeführt. Benutzer können auf dieses Symbol doppelklicken, um den aktuellen Sitzungsstatus und eine Liste von Anwendungen und Hosts anzuzeigen, die für die Vermittlung über Secure Application Manager angegeben sind.

**Abbildung 76** auf Seite 188 verdeutlicht die Interaktion zwischen einer Clientanwendung und dem Server über das IVE.

1. Zum Starten von Windows Secure Application Manager klicken Benutzer auf die IVE-Menüoption für Secure Application Manager. Das IVE lädt das ActiveX-Steuerelement auf den Clientcomputer herunter. Dieses Steuerelement konfiguriert den Clientcomputer zum Ausführen von clientseitigen Diensten (LSP), um den Anwendungsverkehr zu sichern. Das Statusfenstersymbol für den Secure Application Manager wird im System Tray angezeigt.
2. Der Benutzer startet eine vom Administrator festgelegte Anwendung oder initiiert einen Prozess, der Daten von einem angegebenen Host anfordert. Wenn die Clientanwendung oder der Prozess versucht, eine Verbindung mit der Ressource herzustellen, fängt Secure Application Manager die Anforderung ab.
3. Secure Application Manager leitet den Hostnamen über SSL an das IVE weiter. Das IVE löst den Hostnamen auf und gibt die IP-Adresse des Zielhosts an Secure Application Manager zurück.
4. Secure Application Manager konfiguriert automatisch einen Kanal für die Portumleitung. Dazu verwendet er eine vorher bereitgestellte IP-Adresse für den lokalen Host.



**Abbildung 76: Windows Secure Application Manager**

1. Sie können Secure Application Manager so konfigurieren, dass der Start beim Anmelden eines Benutzers automatisch erfolgt. Benutzer können diese Einstellung über das Menü IVE **System > Preferences** außer Kraft setzen. Wenn der automatische Start deaktiviert ist, muss Secure Application Manager manuell gestartet werden, indem auf die entsprechende Verknüpfung im IVE-Homepagemenu geklickt wird.

## ☑ Festlegen von Anwendungen und Hosts, die mit W-SAM gesichert werden sollen.

Verwenden Sie die Unterregisterkarte **Applications > Secure Application Manager**, um Anwendungen und Hosts festzulegen, für die W-SAM den Datenverkehr sichert. Wenn W-SAM auf einen Client-PC heruntergeladen wird, sind darin die Informationen enthalten, die Sie auf der Unterregisterkarte **Applications > Secure Application Manager** für die Autorisierungsgruppe des Benutzers konfigurieren. Nachdem ein Benutzer<sup>1</sup> Secure Application Manager aufgerufen hat, fängt W-SAM Anforderungen von Clientanwendungen an Server im internen Netzwerk und Anforderungen von auf dem Client ausgeführten Prozessen an interne Hosts ab. Sie definieren diese Ressourcen auf der Unterregisterkarte **Secure Application Manager**, indem Sie zwei Listen konfigurieren:

- Liste **Applications**

Diese Liste enthält Anwendungen, für die W-SAM den Client/Serververkehr zwischen dem Client und dem IVE sichern soll.

- Liste **Hosts**

Diese Liste enthält Hosts, für die W-SAM den Client/Serververkehr zwischen dem Client und dem IVE sichern soll. Beachten Sie, dass Sie, um unter Verwendung von W-SAM mit NetBIOS auf eine Freigabe zuzugreifen, sowohl in der W-SAM-Zugriffssteuerungsliste als auch auf der Seite **Add Hosts** den NetBIOS-Namen des Servers (alphanumerische Zeichenfolge mit bis zu 15 Zeichen) explizit angeben müssen. (Gegenwärtig werden keine Platzhalter unterstützt.)

Wenn das IVE Daten vom W-SAM empfängt, prüft es die serverseitige ACL für Secure Application Manager, um festzustellen, ob die Anforderung für die Unternehmensressource, die auf den zulässigen IP/Port-Kombinationen basiert, weitergeleitet wird. Diese ACL wird über die Unterregisterkarte **Applications** konfiguriert.

### So geben Sie Anwendungen und Hosts an, die mit W-SAM gesichert werden sollen

1. Wählen Sie in der Administratorkonsole das Menü **Authentication & Authorization > Authorization Groups** und anschließend eine Gruppe aus.
2. Wählen Sie aus den Gruppenregisterkarten **Applications > General** aus. Vergewissern Sie sich, dass die Windows-Version von Secure Application Manager aktiviert ist.

---

1. Sie können Secure Application Manager so konfigurieren, dass der Start beim Anmelden eines Benutzers automatisch erfolgt. Benutzer können diese Einstellung über das Menü **IVE System > Preferences** außer Kraft setzen. Wenn der automatische Start deaktiviert ist, muss Secure Application Manager manuell gestartet werden, indem auf die entsprechende Verknüpfung im IVE-Homepagemenu geklickt wird.

3. Wählen Sie aus den Gruppenregisterkarten **Applications > Secure Application Manager** aus.

Benutzerdefinierte Autorisierungsgruppen erben standardmäßig die Einstellungen der Benutzergruppe. Klicken Sie zum Festlegen benutzerdefinierter Einstellungen auf **Use custom settings** und anschließend auf **Update**.

4. Geben Sie auf der Liste **Applications** Ressourcen an, für die W-SAM den Client/Server-Verkehr zwischen dem Client und dem IVE sichert:
  - 1 Klicken Sie auf **Add Application**.
  - 2 Geben Sie den Dateinamen der auszuführenden Anwendung ein.
  - 3 Geben Sie den MD5-Hash der auszuführenden Datei ein. (Optional.)

Wenn Sie diesen Wert eingeben, überprüft W-SAM, ob der Prüfsummenwert der ausführbaren Datei diesem Wert entspricht. Wenn die Werte nicht übereinstimmen, teilt W-SAM dem Benutzer mit, dass die Identität der Anwendung nicht sichergestellt werden konnte, und leitet Verbindungen von der Anwendung zum IVE nicht weiter.
  - 4 Geben Sie einen Namen und eine Beschreibung an, die für Benutzer auf der Seite **Applications > Session** angezeigt wird. (Optional.)
  - 5 Klicken Sie auf **Add**.
5. Geben Sie auf der Liste **Hosts** Ressourcen an, für die W-SAM den Client/Server-Verkehr zwischen dem Client und dem IVE sichert:
  - 1 Klicken Sie auf **Add Hosts**.
  - 2 Geben Sie den Hostnamen (die Platzhalterzeichen „\*“ oder „?“ sind zulässig) oder ein IP/Netzmaske-Paar an. Geben Sie mehrere Ports für einen Host als separate Einträge an.
  - 3 Klicken Sie auf **Add**.

---

**Hinweis:** Sie müssen der Secure Application Manager-Zugriffssteuerungsliste jeden in der Liste **Hosts** angegebenen Host hinzufügen. (Beachten Sie den nächsten Schritt.)

---

6. Legen Sie in der Zugriffssteuerungsliste von Secure Application Manager fest, an welche Unternehmensressourcen (basierend auf der Kombination aus IP-Adresse und Port) das IVE eine Anwendungs- oder Hostanforderung senden kann. So konfigurieren Sie diese Zugriffssteuerungsliste
  - 1 Wählen Sie die Unterregisterkarte **Applications > General** aus.
  - 2 Klicken Sie unter **Enable Secure Application Manager** in der aktivierten W-SAM-Option (entweder **Enabled using the Windows version** oder **Enabled using the Windows version with Netbios support**) auf die Verknüpfung **Access Control**.

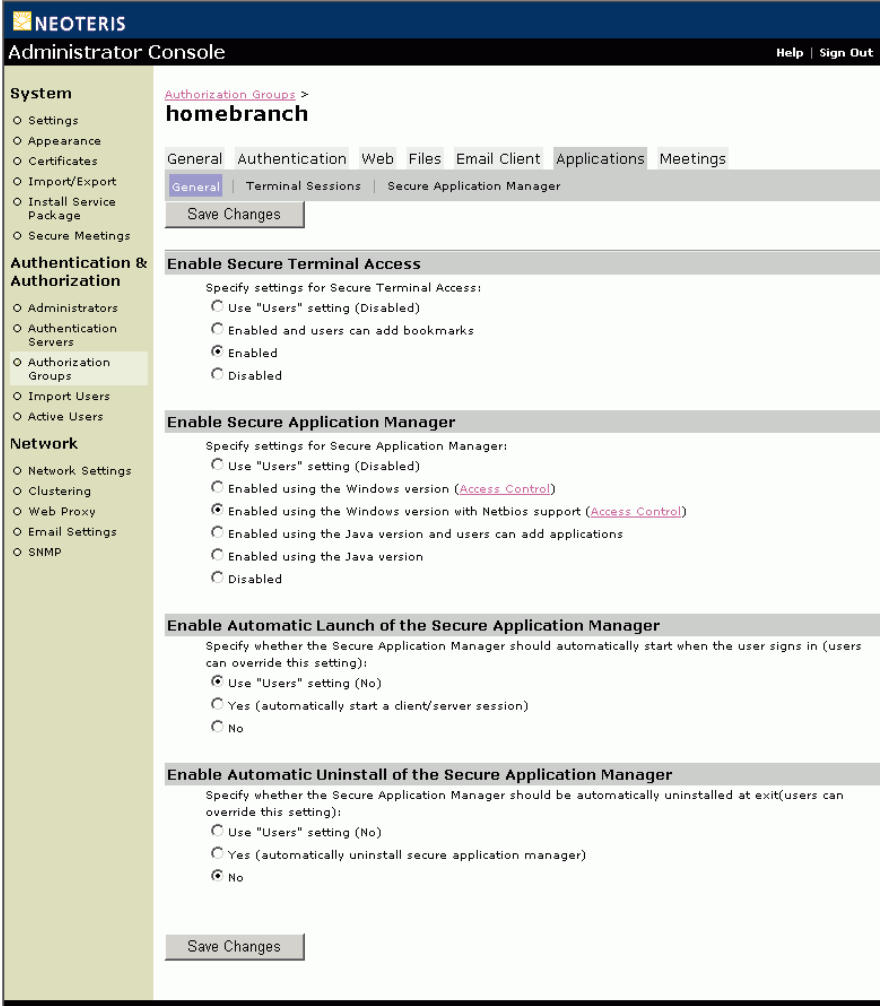


Abbildung 77: Authentication & Authorization > Authorization Groups > GroupName > Applications > General (Windows-Version)

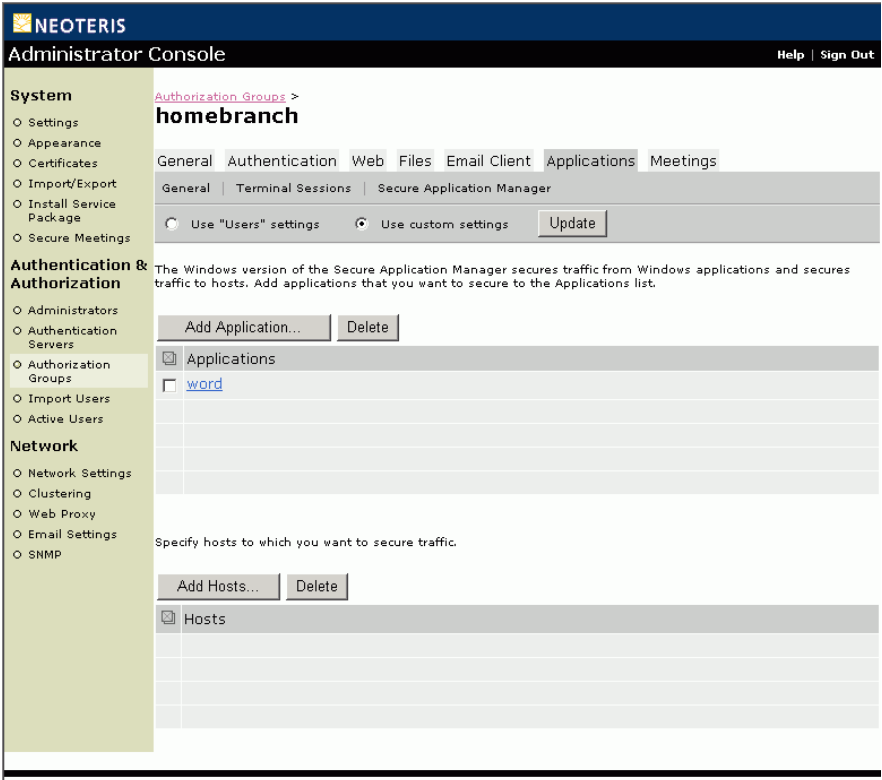


Abbildung 78: Authentication & Authorization > Authorization Groups > GroupName > Applications > Secure Application Manager (Windows-Version)



## Applications > Unterregisterkarte „Secure Application Manager (J-SAM)“

Die Secure Application Manager-Aktualisierungsoption stellt sicheren Remotezugriff auf Anwendungsebene von Clientanwendungen auf Unternehmensserver bereit. Sie können zwei Versionen von Secure Application Manager bereitstellen:

- **Windows-Version (W-SAM)**

Die Windows-Version von Secure Application Manager ist eine Windows-32-Lösung für sicheres, transparentes Umleiten von ausgehenden TCP-Verbindungen über ein IVE-Gerät für jeweils eine Anwendung oder einen Host. Die Software wird von einem im IVE gehosteten ActiveX-Steuerelement heruntergeladen und gestartet.

Weitere Informationen zu W-SAM finden Sie unter „Applications > Unterregisterkarte „Secure Application Manager (W-SAM)““ auf Seite 187.

- **Java-Version (J-SAM)**

Die Java-Version von Secure Application Manager bietet Unterstützung für statische TCP-Port-Client/Server-Anwendungen, darunter erweiterte Unterstützung für Microsoft MAPI, Lotus Notes und Citrix NFuse. Diese Version funktioniert in vielen Netzwerkkonfigurationen einwandfrei, unterstützt jedoch keine Client/Server-Anwendungen auf dynamischer TCP-Port-Basis oder vom Server initiierte Verbindungen.

---

**Hinweis:** Gegenwärtig wird auf Windows- oder Linux-Plattformen Sun JVM Version 1.4.1 oder höher unterstützt.

---

## Übersicht über Java Secure Application Manager (J-SAM)

Die Java-Version von Secure Application Manager (J-SAM) bietet sichere Portweiterleitung für Anwendungen, die auf einem Remotecomputer ausgeführt werden. Das IVE weist jedem Anwendungsserver, den Sie für einen bestimmten Port festlegen, eine eindeutige IP-Loopbackadresse zu. Wenn Sie beispielsweise für einen einzigen Port folgendes festlegen:

app1.mycompany.com, app2.mycompany.com, app3.mycompany.com, ...

weist das IVE jeder Anwendung eine eindeutige IP Loopbackadresse zu:

127.0.1.10, 127.0.1.11, 127.0.1.12, ...

Wenn ein Benutzer J-SAM herunterlädt, überwacht J-SAM die vom IVE zugewiesenen Loopbackadressen (am entsprechenden, für den Anwendungsserver festgelegten Clientport) auf Clientanforderungen an Netzwerkanwendungsserver. J-SAM kapselt die Anforderungsdaten und leitet die verschlüsselten Daten als SSL-Verkehr an das IVE weiter. Das IVE entkapselt die Daten und leitet sie an den festgelegten Serverport auf dem Anwendungsserver im Netzwerk weiter. Der Anwendungsserver gibt seine Antwort an das IVE weiter, das die Daten entkapselt und sie an J-SAM weiterleitet. J-SAM entkapselt dann die Antwort des Servers und leitet die Daten an die Clientanwendung weiter. Für die auf dem lokalen Computer ausgeführte Clientanwendung fungiert J-SAM als Anwendungsserver. Für den Anwendungsserver in Ihrem Netzwerk übernimmt das IVE die Rolle der Clientanwendung.

Damit diese Lösung funktioniert, muss eine Clientanwendung auf dem Computer des Benutzers den Anwendungsserver zu sich selbst – lokaler Host – auflösen, damit J-SAM die über das IVE für den Anwendungsserver bestimmten Daten erfassen und sicher über einen Port weiterleiten kann. Je nach Betriebssystem löst eine Clientanwendung den Hostnamen eines Servers auf dem lokalen Computer unterschiedlich auf. Für:

- **Windows-Benutzer**

kann J-SAM eine automatische Hostzuordnung durchführen und dabei die lokale Datei hosts so bearbeiten, dass dem lokalen Host ein Anwendungsserver zugeordnet wird. J-SAM kann die Datei hosts eines PC-Benutzers nur bearbeiten, wenn der Benutzer auf seinem Computer über Administratorrechte verfügt. Alternativ:

- Sie können Ihren externen DNS-Server zum Auflösen von Anwendungsservern zum lokalen Host konfigurieren. (Siehe Hinweis.)
- Benutzer können eine Clientanwendung so konfigurieren, dass die vom IVE zugewiesene Adresse des lokalen Hosts an der Stelle verwendet werden kann, an der sie normalerweise den Hostnamen des Anwendungsservers eingeben. (Siehe Hinweis.)

- **Linux (RedHat)-Benutzer**

J-SAM kann keine automatische Hostzuordnung durchführen, weil J-SAM keine Berechtigung zum Bearbeiten der Datei hosts besitzt. Nur root verfügt über die Berechtigung zum Ändern der Datei hosts. Für Linux-Benutzer gibt es u. a. folgende Alternativen:

- Sie können Ihren externen DNS-Server zum Auflösen von Anwendungsservern zum lokalen Host konfigurieren. (Siehe Hinweis.)
- Benutzer können eine Clientanwendung so konfigurieren, dass die vom IVE zugewiesene Adresse des lokalen Hosts an der Stelle verwendet werden kann, an der sie normalerweise den Hostnamen des Anwendungsservers eingeben. (Siehe Hinweis.)

## Hinweis:

- Wenn Sie Ihren externen DNS-Server so konfigurieren, dass er eine lokale Hostadresse anstelle des Hostnamens des Anwendungsservers verwendet, müssen Remotebenutzer die Reihenfolge, in der ihr Computer nach DNS-Servern sucht, so konfigurieren, dass mit der Firmen-DNS begonnen wird.
- Weil Benutzer für Anwendungen, die sie für Portweiterleitung hinzufügen, den DNS-Firmenserver nicht ändern können, müssen sie die Anwendung so konfigurieren, dass diese die vom IVE zugewiesene Adresse des lokalen Hosts für den festgelegten Clientport verwendet. Im Fensterausschnitt **Details** des J-SAM-Browserfensters wird die vom IVE zugewiesene IP-Loopbackadresse zusammen mit dem vom Benutzer festgelegten Port angezeigt.
- Linux-Benutzer haben keinen Zugriff auf Ports unter 1024, wenn sie auf Ihrem Computer nicht als root angemeldet sind. Wenn Linux-Benutzer Anwendungen wie Telnet- und Browseranwendungen, die Ports unterhalb von 1024 benötigen, über einen Port weiterleiten möchten, müssen sie eine der folgenden Aktionen ausführen:

- Starten des Browsers, der J-SAM als root startet.
- Angeben einer Client-Portnummer (größer oder gleich 1024) beim Hinzufügen der Anwendung zur Liste **Client Applications**. Nach dem Hinzufügen der Anwendung müssen Benutzer J-SAM starten und im Fensterausschnitts **Details** ablesen, welche IP-Loopbackadresse dem Anwendungsserver zugewiesen wurde. Benutzer müssen diese Adressen-/Portinformationen dann in die Clientanwendung eingeben oder sie an der Befehlszeile verwenden.

Wenn ein Benutzer beispielsweise den Clientport 2041 und den Serverport 23 für eine Telnet-Anwendung festlegt, wird folgender Befehl zum Ausführen der Anwendung verwendet:

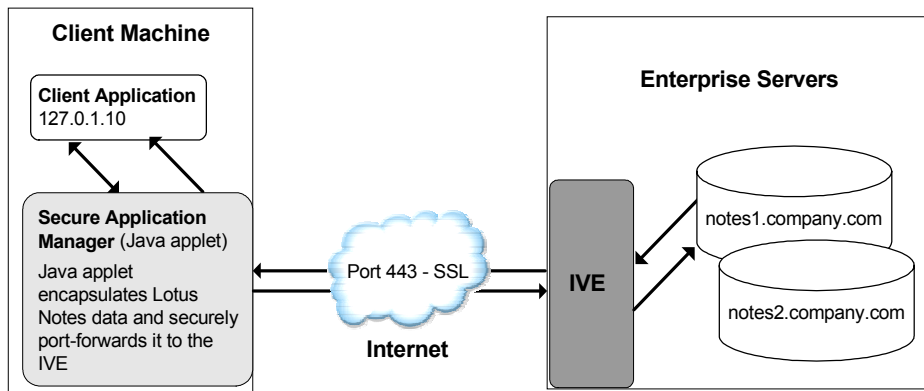
```
telnet loopbackIP 2041
```

J-SAM überwacht Port 2041 auf Datenverkehr von der Telnet-Anwendung und leitet diesen an das IVE weiter. Das IVE leitet den Datenverkehr dann an Port 23 auf dem Zielservers weiter.

**Abbildung 79** auf Seite 196 verdeutlicht die Interaktion zwischen einer Clientanwendung und dem Server über das IVE. In dieser Abbildung wird vorausgesetzt, dass Benutzer eine IP-Adresse des lokalen Hosts als Server in der Clientanwendung festlegen. Wenn Sie das IVE für die Verwendung der automatischen Hostzuordnung (für PC-Benutzer) konfigurieren, beachten Sie **Abbildung 82** auf Seite 206.

1. Der Benutzer startet eine auf der Seite **Client Applications** des IVE aufgeführte Clientanwendung. Die Anwendung löst den Remoteserver zum lokalen Host auf.

2. Die Clientanwendung nimmt Verbindung mit dem auf dem Computer des Benutzers ausgeführten J-SAM auf und beginnt mit dem Senden von Anforderungen.
3. J-SAM kapselt alle Clientanforderungen und leitet diese über SSL an das IVE weiter.
4. Das IVE entkapselt die Clientdaten und leitet sie zum festgelegten Anwendungsserver weiter.
5. Der Anwendungsserver antwortet mit Daten an den IVE-Server.
6. Das IVE kapselt die Antwort und leitet die Antwort vom Anwendungsserver über SSL an J-SAM weiter.
7. J-SAM entkapselt die Anwendungsserverdaten und leitet sie an die Clientanwendung weiter.



**Abbildung 79: Java Secure Application Manager**

In dieser Abbildung wird vorausgesetzt, dass Benutzer eine IP-Adresse des lokalen Hosts als Server in der Clientanwendung festlegen.

## ☑ Festlegen von Clientanwendungen, für die J-SAM eine Portweiterleitung durchführt

Verwenden Sie die Unterregisterkarte **Applications > Secure Application Manager**, um Anwendungen anzugeben, die von J-SAM über einen Port weitergeleitet werden sollen. Wenn J-SAM auf einen Clientcomputer heruntergeladen wird, sind darin die Informationen enthalten, die Sie auf der Unterregisterkarte **Applications > Secure Application Manager** für die Autorisierungsgruppe des Benutzers konfigurieren. Wenn ein Benutzer auf **Client Applications** klickt, wird J-SAM ausgeführt, fängt die Anforderungen an den festgelegten Ports ab und leitet sie über Ports an das IVE weiter. Das IVE leitet die Daten dann an den für den Anwendungsserver festgelegten Port weiter.

---

**Hinweis:** Gegenwärtig wird auf Windows- oder Linux-Plattformen Sun JVM Version 1.4.1 oder höher unterstützt.

---

Falls Sie eine der erweiterten Anwendungen (Microsoft Outlook, Lotus Notes oder Citrix NFuse) aktivieren möchten, müssen Sie diesen Vorgang nicht durchführen. Informationen zu den einzelnen erweiterten Anwendungen finden Sie im entsprechenden Abschnitt:

- MS Outlook—Seite 207
- Lotus Notes—Seite 211
- Citrix NFuse—Seite 215

### So legen Sie die Clientanwendungen fest, für die J-SAM eine Portweiterleitung durchführen soll

1. Wählen Sie in der Administratorkonsole das Menü **Authentication & Authorization > Authorization Groups** und anschließend eine Gruppe aus.
2. Wählen Sie aus den Gruppenregisterkarten **Applications > General** aus. Vergewissern Sie sich, dass die Java-Version von Secure Application Manager aktiviert ist.
3. Wählen Sie aus den Gruppenregisterkarten **Applications > Secure Application Manager** aus.  
Benutzerdefinierte Autorisierungsgruppen erben standardmäßig die Einstellungen der Benutzergruppe. Klicken Sie zum Festlegen benutzerdefinierter Einstellungen auf **Use custom settings** und anschließend auf **Update**.
4. Geben Sie eine Anwendung an, die Remotebenutzer für die Kommunikation mit Netzwerkservers ausführen können:

- 1 Geben Sie den Namen der Anwendung und bei Bedarf eine Beschreibung ein. Diese Informationen werden auf der Seite **Client Applications** für IVE-Benutzer angezeigt.
  - 2 Geben Sie im Feld **Remote Server** den DNS-Namen oder die IP-Adresse des Servers ein.
  - 3 Geben Sie im Feld **Client Port** den Port ein, den J-SAM auf Clientanwendungsverbindungen überwachen soll. Normalerweise stimmt der Wert für den Clientport mit dem für den Serverport überein. Der Wert für den Clientport unterscheidet sich normalerweise nur für Linux-Benutzer, die Anwendungen für Portweiterleitung hinzufügen möchten, die Ports unter 1024 verwenden. Weitere Informationen finden Sie im Hinweis auf Seite 195.  
  
Sie können mehrere Anwendungen an einem einzigen Port konfigurieren, z. B. anw1.meinefirma.com, anw2.meinefirma.com, anw3.meinefirma.com. Das IVE weist jeder Anwendung eine Loopbackadresse (127.0.1.10, 127.0.1.11, 127.0.1.12) zu. J-SAM überwacht diese Loopbackadressen dann an dem festgelegten Port. Wenn beispielsweise Datenverkehr für die Adresse 127.0.1.12 am angegebenen Port vorhanden ist, leitet das IVE den Datenverkehr an den Zielhost anw3.meinefirma.com weiter.
  - 4 Geben Sie im Feld **Server Port** den Port ein, an dem der Remoteserver die Clientverbindungen überwacht.  
  
Wenn beispielsweise Telnet-Verkehr von einem Remotecomputer weitergeleitet werden soll, legen Sie sowohl für den Clientport (an dem J-SAM überwacht) als auch für den Serverport (an dem der Telnet-Server überwacht) Port 23 fest.
  - 5 Aktivieren Sie das Kontrollkästchen **Allow proxy to dynamically select an available port...**, wenn J-SAM am gleichen Port Daten für mehrere Hosts überwacht und einen verfügbaren Port auswählen soll, falls der von Ihnen angegebene Clientport belegt ist. Um diese Option verwenden zu können, muss es die Clientanwendung ermöglichen, die Portnummer für die Verbindung festzulegen.
  - 6 Klicken Sie auf **Add**. Die Anwendung wird auf der IVE-Seite **Client Applications** angezeigt.
5. Wählen Sie aus den Gruppenregisterkarten **Applications > General** aus.
6. Wählen Sie unter **Enable Automatic Host Mapping (Java Version Only)** die Option **Enabled** aus, und klicken Sie dann auf **Save Changes**, wenn es sich bei den Benutzern um PC-Benutzer handelt.

Clientanwendungen müssen Anwendungsserver zur IP-Adresse eines lokalen Hosts auflösen. Wenn Sie die automatische Hostzuordnung für Benutzer von Remote-PCs nicht aktivieren möchten oder wenn es sich bei Ihren Benutzern um Linux-Benutzer handelt, müssen Sie Ihren externen DNS-Server zum Auflösen von Anwendungsservernamen zum lokalen Host eines Benutzers konfigurieren. Detaillierte Informationen finden Sie unter „Konfigurieren der externen DNS-Server und Benutzercomputer (falls erforderlich)“ auf Seite 201.

7. Wenn der PC eines Remotebenutzers für die Verwendung eines Webproxys in Internet Explorer eingerichtet ist, konfigurieren Sie den Clientcomputer so, dass der Proxyserver umgangen wird, wenn der Benutzer Anwendungen startet, die eine Verbindung mit Secure Application Manager herstellen müssen. Weitere Informationen erhalten Sie unter „Konfigurieren eines PCs, der die Verbindung mit dem IVE über einen Proxywebserver herstellt“ auf Seite 202.
8. Fügen Sie dem IVE DNS-Domänen hinzu, wenn Sie über mehrere interne Domänen verfügen (zum Beispiel firma-a.com und firma-b.com), so dass Namen wie zum Beispiel anw1.firma-a.com und anw2.firma-b.com ordnungsgemäß aufgelöst werden:
  - 1 Klicken Sie auf das Menü **Network > Network Settings**.
  - 2 Fügen Sie unter **DNS Name Resolution** im Feld **DNS Domains** eine durch Kommas getrennte Liste der Domänen hinzu.
  - 3 Klicken Sie auf **Save Changes**.

## Zusätzliche Aufgaben für J-SAM

In diesem Abschnitt werden Aufgaben beschrieben, die Sie je nach den für J-SAM konfigurierten Client-/Serveranwendungen und dem von Ihren Benutzern verwendeten Betriebssystem möglicherweise durchführen müssen. Weiterhin enthält der Abschnitt Anweisungen zum Testen von J-SAM in Ihrem Unternehmen.

### Folgende Themen werden behandelt:

- Konfigurieren der externen DNS-Server und Benutzercomputer (falls erforderlich) (201)
- Konfigurieren eines PCs, der die Verbindung mit dem IVE über einen Proxywebserver herstellt (202)
- Testen von J-SAM im Unternehmen (203)

- Import Users
- Active Users

**Network**

- Network Settings
- Clustering
- Web Proxy
- Email Settings
- SNMP

### Enable Secure Application Manager

Specify settings for Secure Application Manager:

- ☐ Use "Users" setting (Disabled)
- ☐ Enabled using the Windows version ([Access Control](#))
- ☐ Enabled using the Windows version with Netbios support ([Access Control](#))
- ☒ Enabled using the Java version and users can add applications
- ☐ Enabled using the Java version
- ☐ Disabled

### Enable Automatic Launch of the Secure Application Manager

Specify whether the Secure Application Manager should automatically start when the user signs in (users can override this setting):

- ☒ Use "Users" setting (No)
- ☐ Yes (automatically start a client/server session)
- ☐ No

### Enable Automatic Uninstall of the Secure Application Manager

Specify whether the Secure Application Manager should be automatically uninstalled at exit (users can override this setting):

- ☐ Use "Users" setting (No)
- ☐ Yes (automatically uninstall secure application manager)
- ☒ No

### Enable Microsoft Exchange

Specify settings for Microsoft Exchange:

- ☒ Use "Users" setting (Enabled with access control (Specify allowed [MS Exchange Servers](#)))
- ☐ Enabled with access control (Specify allowed [MS Exchange Servers](#))
- ☐ Enabled
- ☐ Disabled

### Enable Lotus Notes

Specify settings for Lotus Notes:

- ☐ Use "Users" setting (Enabled with access control (Specify allowed [Lotus Notes Servers](#)))
- ☐ Enabled with access control (Specify allowed [Lotus Notes Servers](#))
- ☐ Enabled
- ☒ Disabled

### Enable Citrix NFuse Integration

Specify settings for Citrix NFuse:

- ☐ Use "Users" setting (Disabled)
- ☐ Enabled (go to [NFuse settings](#) to configure integration parameters.)

Note: Enabling this option will make Citrix ICA files cacheable by web browser.

- ☒ Disabled

### Enable Automatic Host Mapping (Java version only)

Specify whether the Secure Application Manager should automatically map application servers to the client PC for secure port forwarding. This setting does not apply to MS Exchange, Lotus Notes, or Citrix NFuse.

- ☒ Use "Users" setting (Enabled (automatically edit local hosts file))
- ☐ Enabled (automatically edit local hosts file)

Note: Enabling this option requires that users have Administrator privileges on their workstations, and in exceptional circumstances, may leave the user's hosts file in a modified state.

- ☐ Disabled (map hosts via external DNS server)

Note: Add the appropriate entries to your external DNS server.

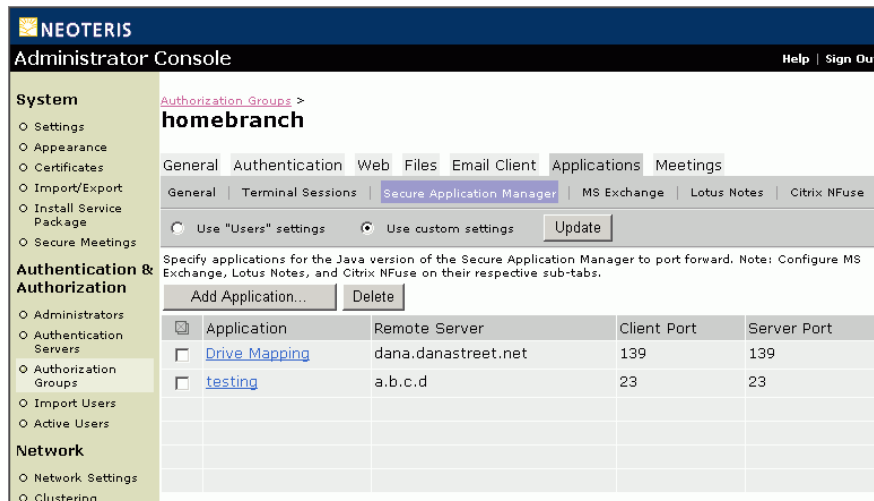
### Enable Automatic Host Mapping for MS Exchange Servers (Java Version Only)

Specify whether to automatically map MS Exchange server names to the client PC for secure MAPI sessions:

- ☒ Use "Users" setting (Enabled (automatically edit local hosts file))
- ☐ Enabled (automatically edit local hosts file)

**Abbildung 80: Authentication & Authorization > Authorization Groups > GroupName > Applications > General (Java-Version)**





**Abbildung 81: Authentication & Authorization > Authorization Groups > GroupName > Applications > Secure Application Manager (Java-Version)**

## ☑ Konfigurieren der externen DNS-Server und Benutzercomputer (falls erforderlich)

Clientanwendungen müssen Hostnamen von Servern zu J-SAM auflösen, wodurch Daten zwischen einem Client und einem Server über einen Proxy gesendet werden. Auf Windows-PCs werden Hostnamen von Servern in der Datei `hosts` gespeichert. Damit Daten mit J-SAM abgefangen werden können, müssen die Servernamen in dieser Datei zur Adresse des lokalen Computers (`localhost`) aufgelöst werden, so dass das IVE den Datenverkehr vermitteln kann. Die empfohlene Vorgehensweise bei der Zuordnung von Anwendungsservern zum lokalen PC eines Benutzers besteht im Aktivieren der automatischen Hostzuordnung (siehe Seite 183). Hierdurch erhält das IVE die Möglichkeit, die Datei `hosts` des PCs so zu ändern, dass Anwendungsserver auf den lokalen Host des PCs verweisen, um eine sichere Portweiterleitung zu gewährleisten.

Das IVE kann nur automatische Hostzuweisung durchführen, wenn der PC-Benutzer auf dem Computer über Administratorrechte verfügt. Andernfalls müssen Sie sicherstellen, dass die internen Anwendungsservernamen extern zum lokalen Host eines PCs aufgelöst werden. Fügen Sie hierfür entsprechende Einträge zu dem externen, mit dem Internet verbundenen DNS-Server hinzu (siehe folgende Beispiele):

```

127.0.0.1 anw1.firma-a.com
127.0.0.1 anw2.firma-b.com
127.0.0.1 exchange1.firma-a.com
127.0.0.1 exchange1.firma-b.com

```

Wenn die Clientanwendung einen unvollständigen Namen für den Anwendungsserver verwendet, müssen Benutzer DNS-Suffixe angeben, damit der PC das Suffix hinzufügen und für die Namensauflösung eine Verbindung mit dem externen DNS-Server herstellen kann. Ein Beispiel: Ein MS Outlook-Client hat üblicherweise einen unvollständigen Namen für einen MS Exchange-Server. Damit der unvollständige Name in die Adresse 127.0.0.1 aufgelöst werden kann, müssen Benutzer die entsprechenden DNS-Suffixe auf ihren PCs angeben. Das Hinzufügen von Domännennamen wirkt sich nicht auf andere Vorgänge auf dem PC aus, einschließlich der Verwendung der Clientanwendung innerhalb des Unternehmens.

### **So konfigurieren Sie einen Benutzer-PC mit DNS-Suffixen (Windows 2000)**

1. Wählen Sie im **Startmenü** von Windows **Einstellungen > Netzwerk- und DFÜ-Verbindungen > LAN-Verbindung** und dann **Eigenschaften** aus.
2. Wählen Sie **Internetprotokoll (TCP/IP)** aus, und klicken Sie dann auf **Eigenschaften**.
3. Klicken Sie auf **Erweitert** und dann auf die Registerkarte **DNS**.
4. Klicken Sie auf **Diese DNS-Suffixe anhängen** und dann auf **Hinzufügen**.
5. Fügen Sie die internen Domänen Ihres Unternehmens als zusätzliche DNS-Suffixe hinzu.

### **☒ Konfigurieren eines PCs, der die Verbindung mit dem IVE über einen Proxywebserver herstellt**

Dieses Verfahren kann jedoch nur angewendet werden, wenn der PC eines Remotebenutzers so konfiguriert ist, dass in Internet Explorer ein Webproxy verwendet wird. Dieses Verfahren gewährleistet, dass Clientanwendungen eine Verbindung mit Secure Application Manager herstellen, statt zu versuchen, eine Verbindung mit dem Webproxy herzustellen.

### So konfigurieren Sie einen PC, der die Verbindung mit dem IVE über einen Webproxy in Internet Explorer herstellt

1. Wählen Sie in Internet Explorer im Menü **Extras** die Option **Internetoptionen** aus.
2. Klicken Sie auf der Registerkarte **Verbindungen** auf die Schaltfläche **LAN-Einstellungen**.
3. Klicken Sie unter **Proxyserver** auf die Schaltfläche **Erweitert**.
4. Geben Sie unter **Ausnahmen** die Adressen ein, für die kein Proxyserver verwendet werden soll. Geben Sie alle Adressen (Hostnamen und „localhost“) ein, die die Clientanwendung beim Herstellen einer Verbindung über Secure Application Manager verwendet.

#### Beispiele:

Wenn der Anwendungsserver den Namen `anw1.firma.com` hat, geben Sie die folgenden Ausnahmen ein:

`anw1;anw1.firma.com;127.0.0.1`

Wenn der Exchange-Server den Namen `exchange.firma.com` hat, geben Sie die folgenden Ausnahmen ein:

`exchange;exchange.firma.com;127.0.0.1`

### ☒ Testen von J-SAM im Unternehmen

Wenn sich die Benutzer innerhalb Ihres Unternehmens befinden, vermittelt das IVE den Client/Server-Datenverkehr nicht. Das interne DNS-System löst Anwendungsservernamen für Clientanwendungen direkt in die interne IP-Adresse des Anwendungsservers auf. Mit anderen Worten, Clientanwendungen stellen keine Verbindung mit dem auf dem lokalen PC eines Benutzers ausgeführten Secure Application Manager her, sondern tauschen Daten direkt mit Anwendungsservern aus.

Um die fehlerfreie Funktion von J-SAM sicherzustellen, müssen Sie eine externe Netzwerkumgebung simulieren. Sie können dieses Szenario auf einem Test-PC erstellen, indem Sie die folgenden Schritte durchführen (basierend auf Windows 2000):

1. Wählen Sie im **Startmenü** von Windows **Einstellungen > Netzwerk- und DFÜ-Verbindungen** aus.
2. Klicken Sie mit der rechten Maustaste auf **LAN-Verbindung**, und wählen Sie dann **Eigenschaften** aus.
3. Klicken Sie auf **Internetprotokoll (TCP/IP)** und dann auf **Eigenschaften**.

4. Klicken Sie auf die Schaltfläche **Erweitert**.
5. Klicken Sie auf die Registerkarte **WINS**.
6. Klicken Sie auf **NETBIOS über TCP/IP deaktivieren**.

Dieser Schritt verhindert, dass Windows innerhalb des Unternehmens die DNS-Auflösung umgeht und stattdessen mithilfe der WINS-Auflösung den Hostnamen des Anwendungsservers in die richtige interne IP-Adresse auflöst. Eine Clientanwendung stellt eine Verbindung mit Secure Application Manager auf dem lokalen PC her.

---

**Wichtig:** Wenn NetBIOS deaktiviert ist, ist der Druck- und Freigabezugriff unter Windows nicht möglich.

---

7. Klicken Sie dreimal auf **OK**, um die Dialogfelder zu schließen.
8. Wenn Sie keine automatische Hostzuordnung verwenden (Sie haben die externen DNS-Einstellungen geändert und den Benutzer-PCs DNS-Suffixe hinzugefügt), suchen Sie nach der Datei hosts (üblicherweise im Verzeichnis `winnt/system32/drivers/etc/`). Nachdem Sie eine Sicherungskopie der Datei hosts angelegt haben, bearbeiten Sie die Datei und fügen Einträge für die internen Anwendungsserver hinzu, wobei jeder Name in die Adresse 127.0.0.1 aufgelöst wird. Wenn diese Änderungen vorgenommen wurden, löst der PC Anwendungsservernamen ordnungsgemäß in die Adresse 127.0.0.1 auf.
9. Testen Sie die Client-/Serveranwendung, die Sie auf den Unterregisterkarten „Secure Application Manager (J-SAM)“, „MS Exchange“, „Lotus Notes“ und „Citrix NFuse“ konfiguriert haben.
10. Aktivieren Sie anschließend wieder NetBIOS auf der Registerkarte **WINS** im Dialogfeld **Netzwerk- und DFÜ-Verbindungen**.

## Applications > Unterregisterkarte „MS Exchange (J-SAM)“

Die Java-Version von Secure Application Manager unterstützt das systemeigene Microsoft Exchange MAPI-Protokoll (Messaging Application Programming Interface)<sup>1</sup>.

### Erweiterte Unterstützung für MS Exchange

Remotebenutzer können den Microsoft Outlook-Client auf ihren PCs zum Zugreifen auf E-Mail, ihre Kalender und andere Outlook-Funktionen über das IVE verwenden. Dafür müssen keine Änderungen am Outlook-Client vorgenommen werden, und es ist keine Verbindung auf Netzwerkebene, wie z. B. ein VPN, erforderlich. Diese Funktion erfordert die Installation der Microsoft JVM auf dem Client-PC und wird auf PCs unter Windows 2000 (mit Internet Explorer 5.5 oder 6.0) unterstützt. Diese Funktion ist auch kompatibel mit PCs unter Windows 98 (mit Internet Explorer 5.5) oder Windows XP (mit Internet Explorer 6.0).

Damit diese Funktion von Remotebenutzern verwendet werden kann, muss der im Outlook-Client eingebettete Name der Exchange-Server von den Netzwerkeinstellungen des Benutzer-PCs zum lokalen PC (127.0.0.1, die Standard-IP-Adresse des lokalen Hosts) aufgelöst werden, um einen sicheren Datenverkehr für den Outlook-Client zu gewährleisten. Wir empfehlen, dass Sie das IVE für die automatische Auflösung von Exchange Server-Hostnamen zum lokalen Host konfigurieren, indem Sie die Datei `hosts` vorübergehend durch die Option zur automatischen Hostzuordnung auf einem Clientcomputer aktualisieren. Weitere Informationen finden Sie unter „Enable Automatic Host Mapping for MS Exchange Servers (Java Version Only)“ auf Seite 184.

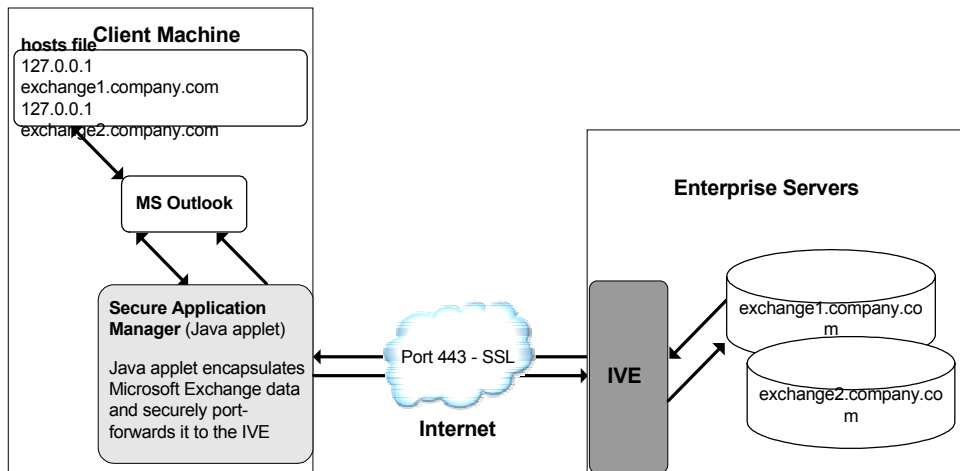
**Abbildung 82** auf Seite 206 beschreibt die Interaktionen zwischen dem Outlook-Client und einem Exchange-Server über das IVE. Diese Abbildung setzt voraus, dass das IVE für die automatische Hostzuordnung konfiguriert ist.

1. Der Benutzer startet den MS Outlook-Client. Outlook versucht, eine Verbindung mit dem Exchange Server `exchange1.ihrefirma.com` herzustellen. Das IVE löst den Hostnamen des Exchange-Servers durch temporäre Änderungen an der Datei `hosts` zu `127.0.0.1` (lokaler Host) auf.
2. Outlook stellt eine Verbindung mit Secure Application Manager her, der auf dem PC des Benutzers ausgeführt wird, und beginnt dann, Anforderungen für E-Mail zu senden.

---

1. Sie können auch die Windows-Version von Secure Application Manager verwenden, um den sicheren Remotezugriff von einem Outlook-Client auf einen MS Exchange-Server zu ermöglichen.

3. Secure Application Manager kapselt alle Anforderungen und leitet diese über SSL vom Outlook-Client an das IVE weiter.
4. Das IVE entkapselt die Clientdaten und sucht in der MAPI-Anforderung nach dem Exchange-Zielserver. Die Anforderung wird dann an den Zielservers weitergeleitet.  
Jede Anforderung im MAPI-Protokoll codiert den Zielservers für die Anforderung. Wenn von Secure Application Managerstammende MAPI-Anforderungen eingehen, werden sie vom IVE-Server überprüft und jeweils zum entsprechenden Zielservers weiterverteilt. Dieser Prozess wird auch bei Vorhandensein mehrerer Exchange-Server unbemerkt ausgeführt.
5. Der Exchange-Server antwortet dem IVE mit E-Mail-Daten.
6. Das IVE kapselt die Antwort und leitet sie vom Exchange-Server über SSL an Secure Application Manager weiter.
7. Secure Application Manager entkapselt die vom IVE gesendeten Informationen und leitet die normale MAPI-Antwort vom Exchange-Server an dem Outlook-Client weiter.



**Abbildung 82: Java Secure Application Manager und erweiterte MS Exchange-Unterstützung**

In dieser Abbildung wird das für die automatische Hostzuordnung für den MS Outlook-Client konfigurierte IVE dargestellt.

## Aktualisierungen der Windows-Registrierung

Beim Start von Secure Application Manager wird die Windows-Registrierungseinstellung `Rpc_Binding_Order` des Benutzers aktualisiert. Diese Einstellung wird der Registrierung hinzugefügt, wenn der Outlook-Client installiert wird, und bestimmt die Protokollsequenz, die der Client zum Kommunizieren mit dem Exchange-Server verwendet.

Der ursprüngliche Wert dieser Einstellung ist:

`ncalrpc,ncacn_ip_tcp,ncacn_spx,ncacn_np,netbios,ncacn_vns_spp`

Nach dem erstmaligen Verwenden von Secure Application Manager ist der Wert: `ncalrpc,ncacn_http,ncacn_ip_tcp,ncacn_spx,ncacn_np,netbios,ncacn_vns_spp`

Die Änderung an `Rpc_Binding_Order` betrifft nur die Ausführung von Secure Application Manager und hat keine anderen Auswirkungen auf dem PC des Benutzers.

---

**Wichtig:** Zum Verwenden des Outlook-Client über die Java-Version von Secure Application Manager müssen Benutzer von Windows-PCs über Administratorrechte verfügen.

---

## ☒ Angeben zulässiger MS Exchange-Server

Verwenden Sie die Unterregisterkarte **Applications > MS Exchange**, um die MS Exchange-Server anzugeben, an die Secure Application Manager Microsoft Outlook-Clientanforderungen weiterleiten kann. Sie müssen diese Registerkarte nur konfigurieren, wenn Sie auf der Unterregisterkarte **Applications > General** die Unterstützung von MS Exchange aktiviert haben (siehe Seite 181).

1. Wählen Sie in der Administratorkonsole das Menü **Authentication & Authorization > Authorization Groups** und anschließend eine Gruppe aus.
2. Wählen Sie aus den Gruppenregisterkarten **Applications > General** aus. Vergewissern Sie sich, dass die Java-Version von Secure Application Manager und die MS Exchange-Optionen aktiviert sind.
3. Wählen Sie aus den Gruppenregisterkarten **Applications > MS Exchange** aus. Benutzerdefinierte Autorisierungsgruppen erben standardmäßig die Einstellungen der Benutzergruppe. Klicken Sie zum Festlegen benutzerdefinierter Einstellungen auf **Use custom settings** und anschließend auf **Update**.

4. Konfigurieren Sie die Zugriffssteuerungsliste für Microsoft Exchange-Server:
  - 1 Geben Sie im Feld **Server Name** den vollständig qualifizierten Hostnamen und den NetBIOS-Namen für jeden MS Exchange Server ein.  
Wenn beispielsweise der vollständig qualifizierte Hostname `exchange1.ihrefirma.com` lautet, fügen Sie der Liste `exchange1.ihrefirma.com` und `exchange1` hinzu.
  - 2 Klicken Sie auf **Add**.
5. Wählen Sie aus den Gruppenregisterkarten **Applications > General** aus.
6. Wählen Sie unter **Enable Automatic Host Mapping for MS Exchange Servers (Java Version Only)** die Option **Enabled** aus, und klicken Sie dann auf **Save Changes**.

Der PC eines Remotebenutzers muss MS Exchange-Server in die Adresse 127.0.0.1 auflösen. Wenn Sie die automatische Hostzuordnung für MS Exchange Server nicht aktivieren möchten, müssen Sie den externen DNS-Server so konfigurieren, dass MS Exchange-Servernamen in die PC-Adresse eines Benutzers aufgelöst werden. Detaillierte Informationen finden Sie unter „Konfigurieren der externen DNS-Server und Benutzercomputer (falls erforderlich)“ auf Seite 201.
7. Wenn der PC eines Remotebenutzers für die Verwendung eines Webproxys in Internet Explorer eingerichtet ist, konfigurieren Sie den Clientcomputer so, dass der Proxyserver umgangen wird, wenn der Benutzer Anwendungen startet, die eine Verbindung mit Secure Application Manager herstellen müssen. Weitere Informationen erhalten Sie unter „Konfigurieren eines PCs, der die Verbindung mit dem IVE über einen Proxywebserver herstellt“ auf Seite 202.



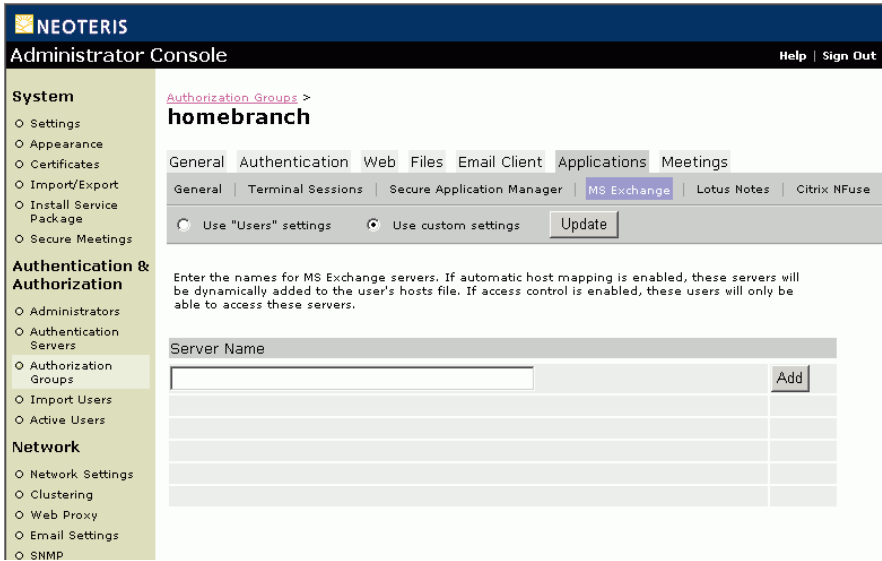


Abbildung 83: Authentication & Authorization > Authorization Groups > GroupName > Applications > MS Exchange (J-SAM)

## Applications > Unterregisterkarte „Lotus Notes (J-SAM)“

Die Java-Version von Secure Application Manager unterstützt das systemeigene Lotus Notes-Protokoll<sup>1</sup>.

### Erweiterte Unterstützung für Lotus Notes

Remotebenutzer können den Lotus Notes-Client auf ihren PCs zum Zugreifen auf E-Mail, ihre Kalender und andere Funktionen über das IVE verwenden. Dafür müssen keine Änderungen am Outlook-Client vorgenommen werden, und es ist keine Verbindung auf Netzwerkebene, wie z. B. ein VPN, erforderlich. Diese Funktion benötigt die Microsoft JVM und wird auf PCs unter Windows 2000 (mit Internet Explorer 5.5 oder 6.0) unterstützt.

Damit Remotebenutzer diese Funktion verwenden können, müssen sie den Lotus Notes-Client zum Verwenden von „localhost“ als Einstellung für den Remotestandort konfigurieren. Secure Application Manager nimmt dann vom Lotus Notes-Client angeforderte Verbindungen auf. In **Abbildung 84** werden die Interaktionen zwischen dem Lotus Notes-Client und einem Lotus Notes-Server über das IVE dargestellt.

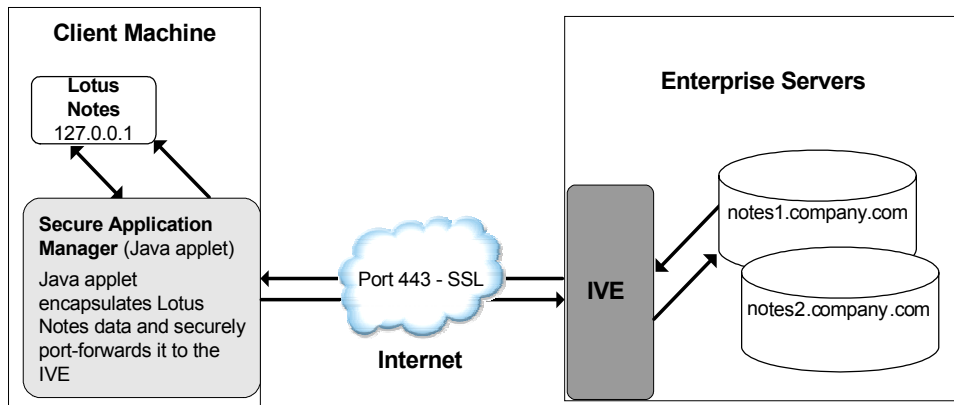
1. Der Benutzer startet den Lotus Notes-Client mit der Home Location-Einstellung. Der Client ermittelt die Proxyeinstellung, d. h. den lokalen Host, den PC des Benutzers, für seine Home Location-Einstellung.
2. Der Lotus Notes-Client stellt eine Verbindung mit Secure Application Manager her, und beginnt damit, Anforderungen für E-Mail zu senden.
3. Secure Application Manager kapselt Anforderungen vom Lotus Notes-Client und leitet diese über SSL an das IVE weiter.
4. Das IVE entkapselt die Clientdaten und ermittelt den Lotus Notes-Zielserver in der Lotus Notes-Anforderung. Die Anforderung wird dann an den Zielserver weitergeleitet.

Jede Anforderung im Lotus Notes-Protokoll codiert den Zielserver für die Anforderung. Wenn Lotus Notes-Anforderungen vom Anwendungsproxy eingehen, ruft der IVE-Server die Zielserverinformationen von den Anforderungen ab und verteilt die Anforderungen an den entsprechenden Zielserver weiter. Deshalb wird diese Funktion auch dann transparent ausgeführt, wenn von einem einzigen Benutzer auf mehrere Lotus Notes-Server zugegriffen wird.

---

1. Sie können auch die Windows-Version von Secure Application Manager verwenden, um den sicheren Remotezugriff von einem Outlook-Client auf einen MS Exchange-Server zu ermöglichen.

5. Der Lotus Notes-Server antwortet dem IVE mit E-Mail-Daten.
6. Das IVE kapselt die Antwort vom Lotus Notes-Server und leitet diese über SSL an Secure Application Manager weiter.
7. Secure Application Manager entkapselt die vom IVE gesendeten Informationen und leitet die normale Antwort vom Lotus Notes-Server an den Lotus Notes-Client weiter.



**Abbildung 84: Java Secure Application Manager und erweiterte Lotus Notes-Unterstützung**

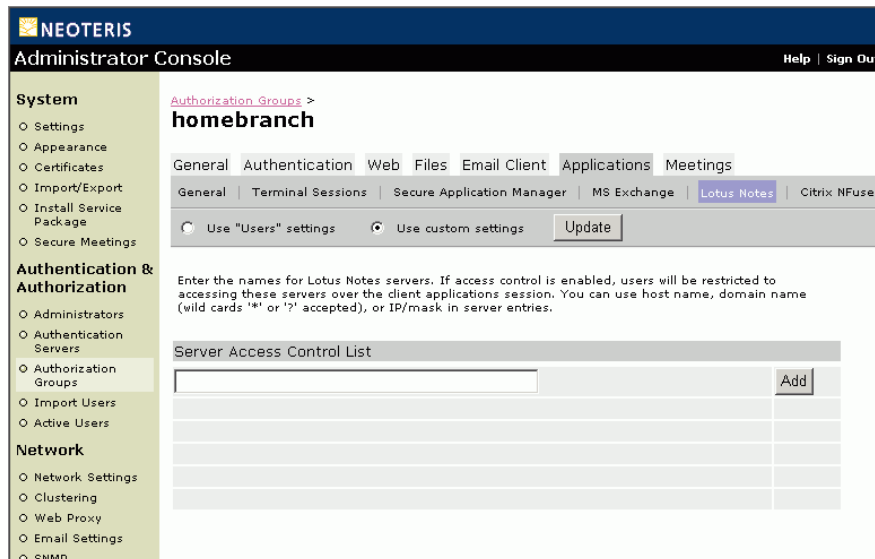
In dieser Abbildung wird der Remotestandortwert des Lotus Notes-Clients dargestellt, der auf dem lokalen Host konfiguriert wird.

## ☒ Festlegen zulässiger Lotus Notes-Server

Verwenden Sie die Unterregisterkarte **Applications > Lotus Notes**, um die Lotus Notes-Server festzulegen, an die Secure Application Manager Lotus Notes-Clientanforderungen weiterleiten kann. Sie müssen diese Registerkarte nur dann konfigurieren, wenn Sie die Unterstützung von Lotus Notes auf der Unterregisterkarte **Applications > General** aktiviert haben (siehe Seite 182).

1. Wählen Sie in der Administratorkonsole das Menü **Authentication & Authorization > Authorization Groups** und anschließend eine Gruppe aus.
2. Wählen Sie aus den Gruppenregisterkarten **Applications > General** aus. Vergewissern Sie sich, dass die Java-Version von Secure Application Manager und die Lotus Notes-Optionen aktiviert sind.

3. Wählen Sie aus den Gruppenregisterkarten **Applications > Lotus Notes** aus. Benutzerdefinierte Autorisierungsgruppen erben standardmäßig die Einstellungen der Benutzergruppe. Klicken Sie zum Festlegen benutzerdefinierter Einstellungen auf **Use custom settings** und anschließend auf **Update**.
4. Konfigurieren Sie die Zugriffssteuerungsliste für Lotus Notes-Server:
  - 1 Geben Sie im Feld **Server Name** den vollständig qualifizierten Hostnamen für jeden MS Exchange-Server ein.  
Wenn beispielsweise der vollständig qualifizierte Hostname `notes1.ihrefirma.com` lautet, fügen Sie der Liste `notes1.ihrefirma.com` und `notes1` hinzu.
  - 2 Klicken Sie auf **Add**.




**Abbildung 85: Authentication & Authorization > Authorization Groups > GroupName > Applications > Lotus Notes (J-SAM)**

## ☑ Konfigurieren des Lotus Notes-Clients

Bevor ein Remotebenutzer von Lotus Notes aus über das IVE eine Verbindung mit einem Lotus Notes-Server herstellen kann, muss der Benutzer den Lotus Notes-Client bearbeiten und ein Adressdokument-Proxyfeld auf den Port des lokalen Hosts für den PC festlegen. Bei dem bearbeiteten Adressdokument sollte es sich um das für den Remotezugriff zu verwendende Dokument handeln, z. B. Home Location oder Travel Location. Wenn das Proxyfeld auf den Port des lokalen Hosts für den PC festgelegt wird, hat das IVE die Möglichkeit, Verbindungen mit mehreren Lotus Notes-Servern herzustellen, einschließlich der als Durchgangsserver konfigurierten Server.

### So konfigurieren Sie einen Lotus Notes-Client für die Verwendung mit dem IVE

1. Wählen Sie auf dem Lotus Notes-Client **File > Mobile > Locations** aus.
2. Wählen Sie den für den Remotezugriff verwendeten Standort aus, und klicken Sie dann auf **Edit Location**.
3. Klicken Sie auf der Registerkarte **Basics** auf das Proxysymbol .
4. Geben Sie im Feld **Proxy Server Configuration** die folgende Adresse in das Feld **HTTP Tunnel** ein: 127.0.0.1:1352
5. Klicken Sie auf **OK**.

Wenn Sie möchten, dass Benutzer dieses Setup durchführen, müssen Sie ihnen die Anweisungen speziell für Ihre Site zur Verfügung stellen.

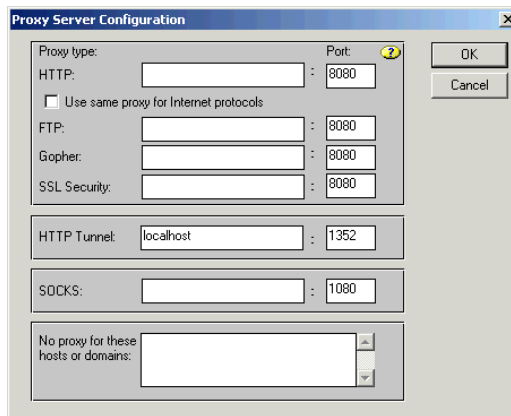


Abbildung 86: Lotus Notes-E-Mail-Client: Dialogfeld „Proxy Server Configuration“

## Applications > Unterregisterkarte „Citrix NFuse (J-SAM)“

Die Java-Version von Secure Application Manager stellt sichere Portweiterleitung von ICA 32-Bit-Windows-Clients an MetaFrame-Server bereit.

### Erweiterte Unterstützung für Citrix NFuse

Wenn ein Benutzer auf einem NFuse-Server eine Anwendung auswählt, sendet der NFuse-Server eine ICA-Datei an den Client. Wenn das IVE die ICA-Datei überschreibt, ersetzt es Hostnamen und IP-Adressen durch vorher bereitgestellte IP-Adressen des lokalen Hosts. Der ICA-Client sendet dann Anwendungsanforderungen an eine der IP-Adressen des lokalen Hosts. Secure Application Manager kapselt die Daten und sendet sie an das IVE. Das IVE entkapselt die Daten und sendet sie über Port 1494 an den passenden MetaFrame-Server.

#### Liste unterstützter Versionen

- MetaFrame™-Server: Versionen 1.8, XP 1.0, mit Service Packs 1 und 2
- Nfuse-Webserver: Versionen 1.5, 1.6 und 1.7
- ICA-Clients:
  - Windows 32-Bit: PN-Client Version 6.30 und Webclient Version 6.3  
Benutzer von Program Neighborhood müssen den Server und die Anwendungen festlegen, auf die sie bei Verwendung des PN-Client zureifen möchten; diese Version des IVE unterstützt den Suchmechanismus nicht, über den Anwendungen auf MetaFrame-Servern für Benutzer von Program Neighborhood angezeigt werden.
  - Java: Version 6.2 für den eigenständigen Client und Versionen 6.2 und 6.3 für den Appletmodus. Wenn Sie den Appletmodus des Java-Client verwenden möchten, müssen Sie darauf achten, dass die Unterstützung für Java-Applets unter „Web > General page“ aktiviert ist.

#### Hinweis:

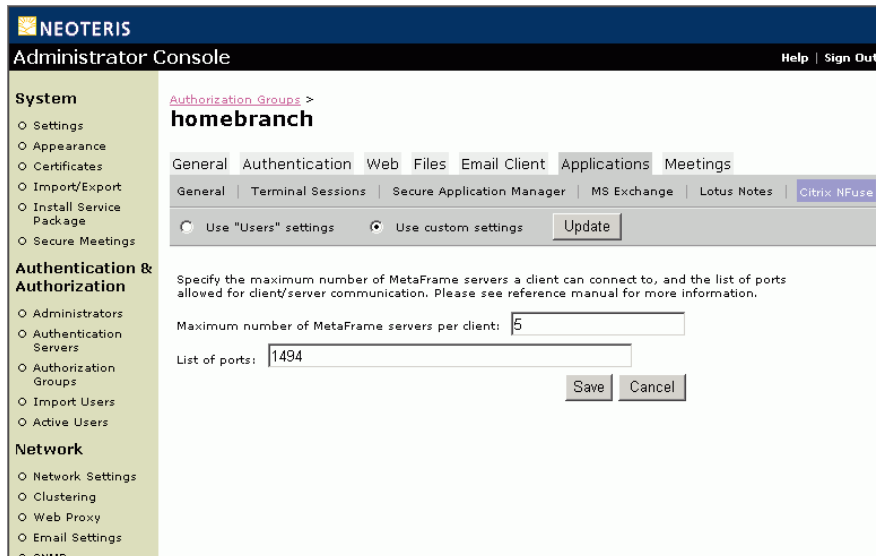
Das IVE stellt eine Alternative zur Bereitstellung von CSG dar.

## ☑ Ändern von Citrix NFuse-Standardeinstellungen

Verwenden Sie die Unterregisterkarte **Applications > Citrix NFuse**, um die Standardeinstellungen für die Integration von Citrix NFuse zu ändern.

### So ändern Sie die Citrix NFuse-Einstellungen

1. Wählen Sie in der Administratorkonsole das Menü **Authentication & Authorization > Authorization Groups** und anschließend eine Gruppe aus.
2. Wählen Sie aus den Gruppenregisterkarten **Applications > General** aus. Vergewissern Sie sich, dass die Java-Version von Secure Application Manager und die Citrix NFuse-Optionen aktiviert sind.
3. Wählen Sie aus den Gruppenregisterkarten **Applications > Citrix NFuse** aus. Benutzerdefinierte Autorisierungsgruppen erben standardmäßig die Einstellungen der Benutzergruppe. Klicken Sie zum Festlegen benutzerdefinierter Einstellungen auf **Use custom settings** und anschließend auf **Update**.
4. Bearbeiten Sie die Standardeinstellungen, und klicken Sie dann auf **Save Changes**. Folgende Optionen stehen zur Verfügung:
  - **Maximum number of MetaFrame servers per client**  
Dieser Wert bestimmt die Anzahl der Citrix MetaFrame-Server, mit denen Benutzer während ihrer Clientanwendungssitzung eine Verbindung herstellen können. Das IVE überwacht MetaFrame-Serveranforderungen an der angegebenen Anzahl von Ports. Benutzer dürfen während ihrer Sitzung nur mit der Höchstzahl der MetaFrame-Server Verbindungen herstellen. Der Standardwert lautet 5.
  - **List of ports**  
Sie können eine durch Kommas getrennte Liste der Ports erstellen, an denen die Citrix MetaFrame-Server Daten überwachen. Der Standardport ist 1494.



**Abbildung 87: Authentication & Authorization > Authorization Groups > GroupName > Applications > Citrix NFuse**

## Registerkarte „Meetings“

### ☑ Ermöglichen und Konfigurieren von Konferenzen für Autorisierungsgruppen

Verwenden Sie diese Registerkarte zu einem beliebigen Zeitpunkt, um festzulegen, welche IVE-Autorisierungsgruppen Konferenzen planen können, um die Sicherheitsstufen für die zu erstellenden Konferenzen zu steuern und um die für Konferenzen verwendeten Systemressourcen zu verwalten.

**Wichtig:** Vor dem Ermöglichen von Konferenzen für Autorisierungsgruppen sollten Sie einen SMTP-E-Mail-Server aktivieren. Folgen Sie dazu den Anweisungen unter „Aktivieren von E-Mail-Benachrichtigungen für Konferenzen“ auf Seite 68.



## So aktivieren und konfigurieren Sie Konferenzen

1. Wählen Sie in der Administratorkonsole das Menü **Authentication & Authorization > Authorization Groups** und anschließend eine Gruppe aus.
2. Wählen Sie aus den Gruppenregisterkarten **Meetings** aus.
3. Wählen Sie eine der folgenden Optionen aus:
  - **User „User“ Settings**  
Wendet Gruppeneinstellungen auf die ausgewählte Autorisierungsgruppe an.
  - **Use custom settings**  
Ermöglicht Ihnen das Festlegen von Konferezeinstellungen für die ausgewählte Autorisierungsgruppe.
4. Klicken Sie auf **Update**. Wenn Sie sich im vorhergehenden Schritt für das Anwenden von Benutzereinstellungen entschieden haben und die Standardeinstellungen für die Benutzergruppe nicht konfigurieren, ignorieren Sie die verbleibenden Anwendungen dieses Abschnitts.
5. Wählen Sie **Enabled** aus, um der in Schritt 1 ausgewählten Autorisierungsgruppe das Planen von Konferenzen zu ermöglichen. Oder wählen Sie **Disabled** aus, um dieser Gruppe das Planen nicht zu ermöglichen. Beachten Sie, dass die Mitglieder der Gruppe dennoch an Konferenzen teilnehmen können, zu denen sie eingeladen sind.
6. Legen Sie das gewünschte Verhältnis zwischen Sicherheit und Verfügbarkeit in Ihren Konferenzen fest, indem Sie im Abschnitt **Security Options** eine der folgenden Optionen auswählen:
  - **Meeting password optional (more accessible)**. Bei Auswahl dieser Option wird dem Ersteller der Konferenz die Entscheidung darüber überlassen, ob für die Teilnahme an der Konferenz ein Kennwort erforderlich ist. Wenn Sie diese Option auswählen, kann jeder, der den URL, die ID-Nummer und das Kennwort (sofern vorhanden) kennt, an der Konferenz teilnehmen, nicht nur IVE-Benutzer.
  - **Require meeting password (more secure)**. Bei Auswahl dieser Option muss der Ersteller der Konferenz entweder ein Kennwort für die Konferenz erstellen oder das von Secure Meeting erzeugte Kennwort verwenden. Wenn Sie diese Option auswählen, kann jeder, der den URL, die ID-Nummer und das Kennwort kennt, an der Konferenz teilnehmen, nicht nur IVE-Benutzer.
  - **Require server-generated password (even more secure)** Bei Auswahl dieser Option muss der Ersteller der Konferenz das von Secure Meeting erzeugte Kennwort verwenden. Wenn Sie diese Option auswählen, kann jeder, der den URL, die ID-Nummer und das Kennwort kennt, an der Konferenz teilnehmen, nicht nur IVE-Benutzer.

- **Require secure gateway authentication (most secure).** Bei Auswahl dieser Option können nur solche eingeladene Benutzer an Konferenzen teilnehmen, die am sicheren IVE-Gateway authentifiziert wurden. Wenn Sie diese Option auswählen, muss der Ersteller der Konferenz kein Kennwort für die Konferenz erstellen, da sich alle Benutzer am sicheren IVE-Gateway authentifizieren müssen.
7. Geben Sie an, ob Sie Vorführenden der Konferenz ermöglichen möchten, die Steuerung ihrer Desktops und Anwendungen mit anderen Teilnehmern der Konferenz zu teilen, indem Sie im Bereich **Security Options** eine der folgenden Optionen auswählen:
- **Allow remote control of shared windows (more functional)** Die Auswahl dieser Option erlaubt dem Vorführenden oder Leiter der Konferenz, die Steuerung des Desktops und der Desktopanwendungen des Vorführenden an einen beliebigen Teilnehmer der Konferenz abzugeben, nicht nur an IVE-Benutzer.
  - **Disable remote control (more secure)** . Die Auswahl dieser Option beschränkt die Steuerung des Desktops und der Desktopanwendungen des Vorführenden der Konferenz ausschließlich auf den Vorführenden selbst.
8. Geben Sie im Bereich **Meeting Policy Settings** an, ob Sie die von Secure Meeting-Benutzern verwendeten Ressourcen einschränken möchten:
- Aktivieren Sie das Kontrollkästchen **Limit number of scheduled meetings**, und geben Sie einen entsprechenden Wert für die maximale Anzahl von Konferenzen ein, die gleichzeitig für die Autorisierungsgruppe geplant werden kann.
  - Aktivieren Sie das Kontrollkästchen **Limit number of simultaneous meetings**, und geben Sie einen entsprechenden Wert für die maximale Anzahl von Konferenzen ein, die gleichzeitig von Mitgliedern der Autorisierungsgruppe abgehalten werden kann.
  - Aktivieren Sie das Kontrollkästchen **Limit number of simultaneous meeting attendees**, und geben Sie einen entsprechenden Wert für die maximale Anzahl von Personen ein, die gleichzeitig an von Mitgliedern der Autorisierungsgruppe geplanten Konferenzen teilnehmen können.
  - Aktivieren Sie das Kontrollkästchen **Limit duration of meetings**, und geben Sie einen entsprechenden Wert (in Minuten) für die maximale Dauer einer Konferenz ein.

---

**Wichtig:** Das IVE begrenzt außerdem die Anzahl von Konferenzen, an denen Benutzer teilnehmen können:

- Ein einzelner Benutzer kann pro Computer nur an einer Konferenz teilnehmen.
- Ein einzelner Benutzer kann innerhalb eines Zeitraums von 3 Minuten an höchstens 10 aufeinander folgenden Konferenzen teilnehmen.

Diese Begrenzungen werden zusätzlich zu den Konferenz- und Benutzerbegrenzungen angewendet, die von Ihrer Secure Meeting-Lizenz definiert wurden.

---

9. Klicken Sie auf **Save Changes**.

Das IVE fügt den sicheren Gateway-Homepages der Benutzer in der festgelegten Autorisierungsgruppe eine Verknüpfung mit der Bezeichnung **Meeting** hinzu.

Informationen zum Anzeigen von Konferenzen, die von Endbenutzern erstellt werden, finden Sie unter „Anzeigen und Absagen geplanter Konferenzen“ auf Seite 70.

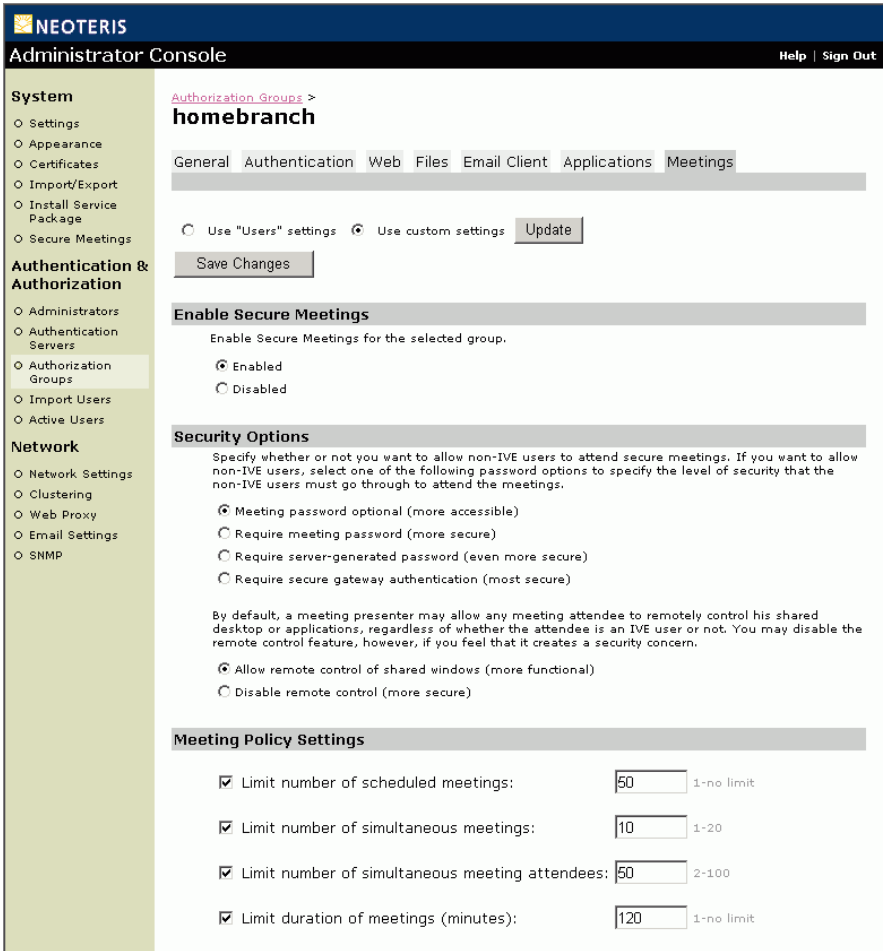


Abbildung 88: Authentication & Authorization > GroupName > Meetings

## Authentication & Authorization > Menü „Import Users“

Auf der Seite **Import Users** können Sie anhand einer einfachen Textdatei problemlos Benutzerdatensätze in das IVE importieren. Mit dieser Funktion können Sie folgende Aktionen durchführen:

- Neue Benutzer über eine einfache Textdatei erstellen
- Vorhandene Benutzerdatensätze wiederverwenden, die von einem anderen System (wie Siebel) exportiert wurden
- Benutzer zu vorhandenen Autorisierungsgruppen hinzufügen
- Neue Autorisierungsgruppen für die neuen Benutzer erstellen

Wenn Sie Benutzer importieren, erstellen Sie einfach eine Textdatei mit Informationen zu den neuen Benutzern, einschließlich ihrer Benutzernamen, Kennwörter, vollständigen Namen und der Autorisierungsgruppen, denen sie zugeordnet werden. Verwenden Sie dann die Verwaltungskonsole, um die Datei der Benutzerdatensätze in den Authentifizierungsserver Ihrer Wahl zu importieren.

### ☒ Erstellen einer Textdatei mit Benutzerdatensätzen

Zum Importieren mehrerer Benutzer auf einmal in den IVE müssen Sie zuerst eine Textdatei mit den neuen Benutzerdatensätzen erstellen, in der die Datensätze in folgendem Format dargestellt werden:

```
Benutzername,Kennwort,vollständiger Name,Gruppe1,Gruppe2,...Gruppen
```

Dabei ist:

- **Benutzername** der Name, den der Benutzer beim Anmelden am IVE eingibt (erforderlich).
- **kennwort** das Kennwort des Benutzers (für auf einen lokalen IVE-Authentifizierungsserver importierte Benutzerdatensätze erforderlich).
- **vollständiger Name** der Vor- und Nachname des Benutzers. Beachten Sie, dass der vollständige Name des Benutzers keine Kommas enthalten darf (wie z. B. „Doe, John“).
- **Gruppe1,Gruppe2,...Gruppen** die Autorisierungsgruppen, denen Benutzer zugeordnet werden sollen (optional).

Beachten Sie beim Erstellen von Textdateien mit Benutzerdatensätzen Folgendes:

- Das IVE unterscheidet in der Datensatzdatei nicht zwischen Groß- und Kleinschreibung. „Joe“ und „joe“ werden vom IVE als ein und derselbe Benutzer behandelt.
- Sie müssen jeden einzelnen Benutzerdatensatz in der Datei in einer eigenen Zeile platzieren und diese mit einem festen Zeilenumbruchszeichen abschließen.
- Jeder Parameter muss von einem Komma gefolgt sein, wobei direkt nach dem Komma, ohne Leerzeichen, der nächste Parameter anschließt. Der erste der beiden folgenden Datensätze ist beispielsweise gültig, der zweite hingegen nicht:

```
sally1,meinkennwort,Sally Reed,DoktorenGruppe,Benutzer
```

```
sally1, meinkennwort, Sally Reed, DoktorenGruppe, Benutzer
```

- Es müssen nicht in jedem Datensatz alle oben beschriebenen Parameter angegeben werden (Benutzername, Kennwort, vollständiger Name, Gruppe). Wenn Sie jedoch einige Parameter angeben und andere nicht, müssen Sie für die nicht angegebenen (Null-)Parameter Kommas einfügen. Wenn Sie z. B. einen neuen Benutzer mit dem Namen „John“ mit dem Kennwort „JohnsKennwort“ erstellen und ihn der Autorisierungsgruppe „Group1“ zuordnen möchten, formatieren Sie den Datensatz wie folgt:

```
John,JohnsKennwort,,Gruppe1
```

Mit dieser Zeile werden der Benutzer und die Gruppe wie beschrieben erstellt, der Parameter für den vollständigen Namen bleibt jedoch leer (wie durch das zusätzliche Komma angezeigt).

- Wenn Sie einen Benutzer mithilfe der Textdatei einer nicht vorhandenen Gruppe zuordnen, erstellt das IVE beim Import eine neue Gruppe mit dem angegebenen Namen. Die Regeln für die Benutzer-zu-Gruppen-Zuordnung für die neue Gruppe werden durch den Authentifizierungsserver bestimmt, auf den die Textdatei importiert wird, und die neue Gruppe wird mit den Standardeinstellungen für „Benutzer“ konfiguriert.
- Wenn Sie einen Benutzer mithilfe der Textdatei einer Gruppe und über den Authentifizierungsserver einer anderen Gruppe zuordnen, erhalten die Zuordnungen des Servers Priorität, und der Benutzer wird der vom Server angegebenen Gruppe zugeordnet. Beachten Sie jedoch, dass das IVE die in der Textdatei angegebenen Benutzer-zu-Gruppen-Zuordnungen speichert. Wenn die Konfiguration des Servers später geändert wird, um Gruppenzuordnungen über die Textdatei zuzulassen (wenn z. B. der Administrator Benutzerzuordnungen zu Gruppen nach Benutzernamen vornehmen möchte), werden die Gruppenzuordnungen in der Textdatei abgerufen und angewendet.

## ☑ Importieren von Benutzer- und Gruppeneinstellungen auf einen Authentifizierungsserver

### So importieren Sie Benutzerdatensätze aus einer Textdatei in das IVE

1. Wählen Sie in der Administratorkonsole das Menü **Authentication & Authorization > Import Users** aus.
2. Geben Sie im Feld **File to import** den Pfad der Textdatei mit den Benutzerdatensätzen ein. Mithilfe der Schaltfläche **Browse** können Sie ggf. zu der Datei auf der Festplatte navigieren.
3. Wählen Sie den **Authentication Server** aus, auf den Sie die Benutzerdatensätze importieren möchten.
4. Um sich die in der Datei enthaltenen Benutzerdatensätze in einer Vorschau anzeigen zu lassen, klicken Sie auf **Preview**. Das IVE zeigt ein Beispiel-Importprotokoll für die Datei an. Wenn Sie die Datei erst nach der Vorschau importieren möchten, müssen Sie die Schritte 2 bis 3 wiederholen.
5. Klicken Sie auf **Import**.

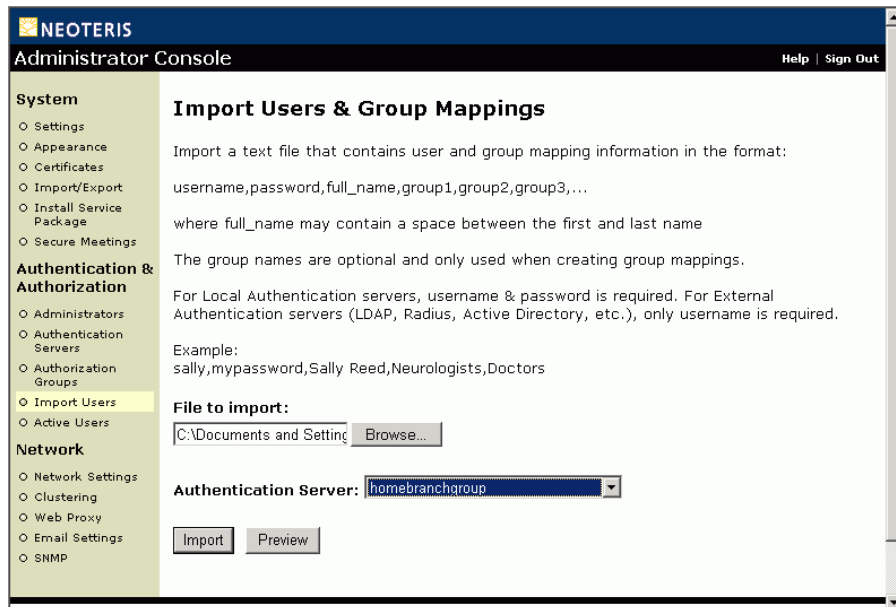


Abbildung 89: Authentication & Authorization > Import Users

## Authentication & Authorization > Menü „Active Users“

### ☒ Überwachen von am IVE angemeldeten Benutzern

Über das Menü **Active Users** können Sie Benutzer überwachen, die am IVE angemeldet sind.

#### **So überwachen Sie am IVE angemeldete Benutzer**

1. Wählen Sie in der Administratorkonsole das Menü **Authentication & Authorization > Active Users** aus.
2. Führen Sie bei Bedarf die folgenden Vorgänge durch:
  - Um die Tabelle der aktuell angemeldeten Benutzer zu sortieren, klicken Sie auf eine Spaltenüberschrift.
  - Um einen oder mehrere Benutzer zwangsweise abzumelden, aktivieren Sie die Kontrollkästchen neben den entsprechenden Benutzernamen, und klicken Sie dann auf **Delete Session**.
  - Um alle aktuell angemeldeten Benutzer zwangsweise abzumelden, klicken Sie auf **Delete All Sessions**.

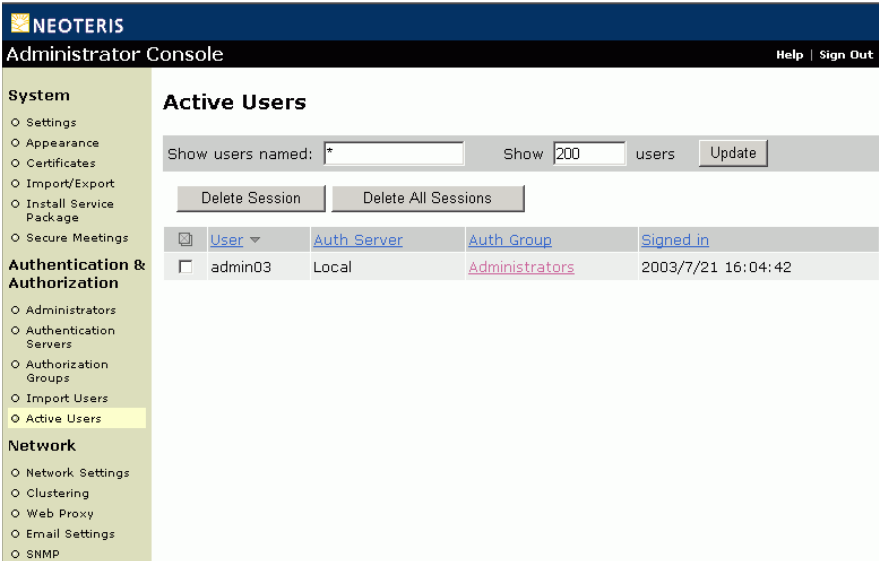


Abbildung 90: Authentication & Authorization > Active Users



## Kapitel4

# Verwalten von IVE Netzwerkeinstellungen

Die Verwaltung des IVE umfasst die Konfiguration und Verwaltung von systemweiten Einstellungen, Authentifizierungsservern, Autorisierungsgruppen und Netzwerkeinstellungen. Dieses Kapitel behandelt Aufgaben, die sich auf das Konfigurieren der IVE-Netzwerkeinstellungen beziehen, und stellt schrittweise Anleitungen zur Durchführung dieser Aufgaben zur Verfügung.

### Übersichtsinformationen finden Sie unter:

Konfigurieren allgemeiner Netzwerkeinstellungen für das IVE .....	226
Konfigurieren eines Clusters von IVE-Servern.....	227
Konfigurieren des IVE als Webproxy .....	233
Konfigurieren der Aktualisierungsoption für Secure Email Client.....	234
Überwachen des IVE als SNMP-Agent.....	239

### Informationen zur Vorgehensweise finden Sie unter:

Network > Menü „Network Settings“ .....	240
Network > Menü „Clustering“ .....	247
Menü „Network > Web Proxy“ .....	264
Menü „Network > Email Settings“ .....	267
Menü „Network > SNMP“ .....	270

---

## Konfigurieren allgemeiner Netzwerkeinstellungen für das IVE

Wenn Sie die Neoteris IVE-Appliance installieren, nehmen Sie grundlegende Einstellungen für die LAN-Verbindung über den internen Port der Appliance vor. Über den internen Port werden alle WAN- und LAN-Anforderungen an jede Ressource abgewickelt, d. h. Webbrowsersabfragen, Dateiabfragen, Authentifizierung und ausgehende Mailanforderungen. Sie können die Appliance auch im Dual-Port-Modus bereitstellen, um eingehende Web- und E-Mail-Proxy-SSL-Verbindungen an einem externen Port abzufragen.

Die externe Schnittstelle fragt nur Anforderungen von Benutzern ab, die am IVE angemeldet sind, und leitet nur deren Anforderungen weiter. Vor dem Senden eines Pakets ermittelt das IVE, ob das Paket einer TCP-Verbindung zugeordnet ist, die von einem Benutzer über die externe Schnittstelle initiiert wurde. Ist dies der Fall, sendet das IVE das Paket an die externe Schnittstelle. Alle übrigen Pakete werden an die interne Schnittstelle gesendet. Die für jede Schnittstelle festgelegten Routen werden verwendet, nachdem das IVE ermittelt hat, ob die interne oder die externe Schnittstelle zu verwenden ist. Das IVE leitet keine Anforderungen von der externen Schnittstelle ein, und diese Schnittstelle akzeptiert keine anderen Verbindungen (mit Ausnahme von Ping- und Tracerouteverbindungen). Alle Anforderungen an eine beliebige Ressource werden von der internen Schnittstelle ausgegeben.

Informationen zur Vorgehensweise:

- Ändern von ursprünglichen Netzwerkeinstellungen, siehe Seite 240.
- Konfigurieren des externen Ports, siehe Seite 241.
- Angeben von statischen Routen, siehe Seite 243.

# Konfigurieren eines Clusters von IVE-Servern

Das IVE, Version 3.1 unterstützt ein Clusterpaar und Multi-Unit-Cluster. Ein **Clusterpaar** besteht aus zwei Neoteris Access 1000-, 3000- oder 5000-Plattformen, die in einer Aktiv/Passiv- oder Aktiv/Aktiv-Konfiguration bereitgestellt werden, um hohe Verfügbarkeit und Lastenausgleich zu gewährleisten. Ein **Multi-Unit-Cluster** besteht aus drei oder mehr Neoteris Access 5000-Plattformen, die in einer Aktiv/Aktiv-Konfiguration bereitgestellt werden, um verbesserte Skalierbarkeit, hohe Verfügbarkeit und gesteigerte Leistung zu bieten.

IVE-Clusterlösungen sind für den Einsatz in einem LAN vorgesehen, in dem alle Clustermitglieder mit dem gleichen Netzwerksegment verbunden sind. Bei diesem Szenario sind alle externen Schnittstellen mit einem Netzwerksegment und alle internen Schnittstellen mit einem anderen Netzwerksegment verbunden. In Version 3.1 wurde die Einsatzmöglichkeit unserer Clusterlösungen auf mehrere Netzwerksegmente (oder ein WAN) ausgeweitet, sodass Clustermitglieder unterschiedliche Netzwerkeinstellungen aufweisen können.

**Wichtig:** Die Zusammenfassung zu Clustern in verschiedenen Netzwerksegmenten ist nur in speziellen Szenarios möglich, in denen Verbindungen auf Netzwerkebene mit niedriger Latenz zwischen den IVEs und den Ressourcen der Back-End-Anwendung besteht. Dieses Feature steht nur als Testversion zur Verfügung.

In diesem Abschnitt erhalten Sie eine Übersicht über Cluster. Informationen zur Vorgehensweise finden Sie unter:

Definieren und Initialisieren eines Clusters .....	247
Hinzufügen eines IVEs zu einem Cluster über die serielle Konsole .....	249
Hinzufügen eines IVEs zu einem Cluster über die Administratorkonsole ...	254
Aktualisieren eines Clusters .....	256
Verwalten von Clusterknoten und Angeben neuer Clustermitglieder .....	257
Ändern von Clustereigenschaften oder Löschen eines Clusters .....	262

## Übersicht über Cluster

Sie legen einen Cluster in einem IVE mithilfe der folgenden drei Angaben fest:

- 1 Eine Bezeichnung für den Cluster
- 2 Ein gemeinsames Kennwort für die Clustermitglieder
- 3 Einen Namen, der das IVE im Cluster kennzeichnet

Nachdem Sie diese Daten auf der Seite **Network > Clustering** angegeben haben, klicken Sie auf **Create Cluster**, um den Cluster zu initiieren und das aktuelle IVE zum Cluster hinzuzufügen. Nach der Definition des Clusters enthält die Seite **Clustering** die Registerkarten **Status** und **Properties**. Der Status des neuen Clusters wird auf der Registerkarte **Status** angezeigt. Die Registerkarte **Status** enthält den Clusternamen und -typ, ermöglicht Ihnen die Angabe neuer Mitglieder sowie die Verwaltung bestehender Mitglieder und bietet umfassende Informationen zum Clusterstatus. **Abbildung 107** auf Seite 259 zeigt die Registerkarte **Status**, die in Tabelle 1 auf Seite 259 detailliert beschrieben wird.

Nach der Definition und Initialisierung eines Clusters müssen Sie angeben, welche IVEs zu dem Cluster hinzugefügt werden. Nachdem ein IVE als vorgesehenes Mitglied angegeben wurde, können Sie es dem Cluster über folgende Komponenten hinzufügen:

- **Serielle Konsole**

Es empfiehlt sich, ein nicht initialisiertes oder eigenständiges IVE einem Cluster über die serielle Konsole (siehe Seite 273) hinzuzufügen, da Sie bei diesem Verfahren nur wenige Angaben für den Beitritt zum Cluster machen müssen.

- **Administratorkonsole**

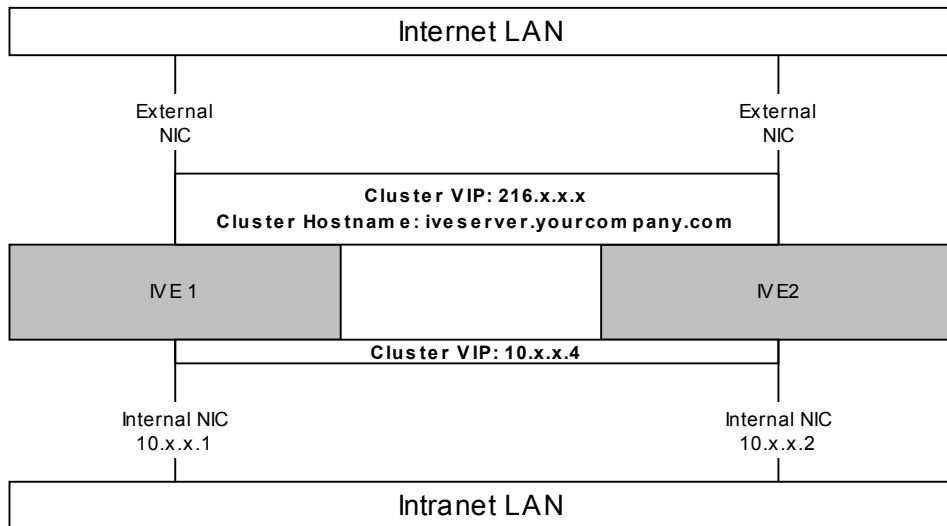
Falls das IVE nicht initialisiert ist, müssen Sie die Ersteinrichtung für das IVE durchführen, bevor Sie es über die Administratorkonsole zu einem Cluster hinzufügen können. Das dem Produkt beiliegende Installationshandbuch enthält Erläuterungen zur Installation und Erstkonfiguration eines IVE. Dieses Handbuch steht auch auf der Neoteris-Support-Site im PDF-Format zur Verfügung.

Wenn ein IVE einem Cluster hinzugefügt wird, initialisiert es seinen Status von einem bestehenden Mitglied, das Sie festlegen. Das neue Mitglied sendet eine Nachricht an das bestehende Mitglied und fordert die Synchronisation an. Das bestehende Mitglied sendet daraufhin den Systemstatus an das neue Mitglied, wodurch *alle* Systemdaten dieses Geräts überschrieben werden. Danach synchronisieren die Mitglieder des Clusters bei jedem Auftreten eines Ereignisses die Daten miteinander. Die Kommunikation zwischen Clustermitgliedern ist verschlüsselt, um Angriffe von außerhalb der firmeninternen Firewall zu verhindern. Jedes IVE verwendet das gemeinsame Kennwort zum Entschlüsseln der Nachrichten von anderen Clustermitgliedern.

## Bereitstellen eines Clusters im Aktiv/Passiv-Modus

Die Neoteris Access 1000-, 3000- und 5000-Plattformen können als Clusterpaar im Aktiv/Passiv-Modus bereitgestellt werden. In diesem Modus bearbeitet ein IVE aktiv Benutzeranforderungen, während das andere IVE passiv im Hintergrund ausgeführt wird, um Statusdaten, einschließlich Systemstatus, Benutzerprofil und Protokollmeldungen, zu synchronisieren. Benutzeranforderungen an die Cluster-VIP werden an das aktive IVE geleitet. Wird das aktive IVE offline geschaltet, beginnt das Standby-IVE automatisch mit der Bearbeitung der Benutzeranforderungen. Benutzer müssen sich nicht neu anmelden, obwohl einige IVE-Sitzungsdaten, wie zum Beispiel Cookies und Kennwörter, möglicherweise nicht auf das aktuelle IVE-Feld synchronisiert wurden. In diesem Fall müssen sich die Benutzer an den Back-End-Webservern neu anmelden.

**Abbildung 91** zeigt eine IVE-Clusterkonfiguration vom Typ Aktiv/Passiv mit zwei IVEs, für die externe Ports aktiviert sind. Beachten Sie, dass dieser Modus weder den Durchsatz noch die Benutzerkapazität erhöht. Er bietet jedoch Redundanz, um auf unerwartete Systemausfälle zu reagieren.



**Abbildung 91: Aktiv/Passiv-Clusterpaar**

Die Abbildung zeigt einen Aktiv/Passiv-Cluster innerhalb des Netzwerks. IVE-Benutzeranforderungen werden an die Cluster-VIP geleitet, die diese dann an das aktive IVE weiterleitet.

## Bereitstellen eines Clusters im Aktiv/Aktiv-Modus

Die Neoteris Access 1000-, 3000- und 5000-Plattformen können als Clusterpaar im Aktiv/Aktiv-Modus bereitgestellt werden. Multi-Unit-Cluster bestehen definitionsgemäß aus mindestens drei Neoteris Access 5000-Plattformen und werden im Aktiv/Aktiv-Modus betrieben.

Im Aktiv/Aktiv-Modus bearbeiten alle IVEs im Cluster aktiv die von einem externen Load-Balancer erhaltenen Benutzeranforderungen. Der Load-Balancer hostet die Cluster-VIP und leitet Benutzeranforderungen auf der Grundlage von SIP-Weiterleitung (Source IP) an ein in seiner Clustergruppe definiertes IVE weiter. Wenn ein IVE offline geschaltet wird, passt der Load-Balancer die Datenlast auf den aktiven IVEs an. Benutzer müssen sich nicht neu anmelden, obwohl einige IVE-Sitzungsdaten, wie zum Beispiel Cookies und Kennwörter, möglicherweise nicht auf das aktuelle IVE-Feld synchronisiert wurden. In diesem Fall müssen sich die Benutzer an den Back-End-Webservern neu anmelden.

Der IVE-Cluster selbst führt keine automatischen Failover- oder Lastenausgleichoperationen durch. Er synchronisiert jedoch Statusdaten (System-, Benutzer- und Protokolldaten) zwischen den Clustermittgliedern. Wenn ein offline geschaltetes IVE wieder online geschaltet wird, passt der Load-Balancer die Datenlast erneut an, um sie auf alle aktiven Mitglieder zu verteilen. Dieser Modus bietet gesteigerten Durchsatz und höhere Leistung während Spitzenlastzeiten, verbessert jedoch die Skalierbarkeit über die Gesamtzahl der lizenzierten Benutzer hinaus nicht.

Das IVE hostet ein CGI, das den Dienststatus für jedes IVE in einem Cluster zur Verfügung stellt. Externe Load-Balancer können anhand dieser Ressource ermitteln, wie die Datenlast effektiv auf die Clusterknoten verteilt werden kann.

Der L7-Überprüfungs-URL lautet:

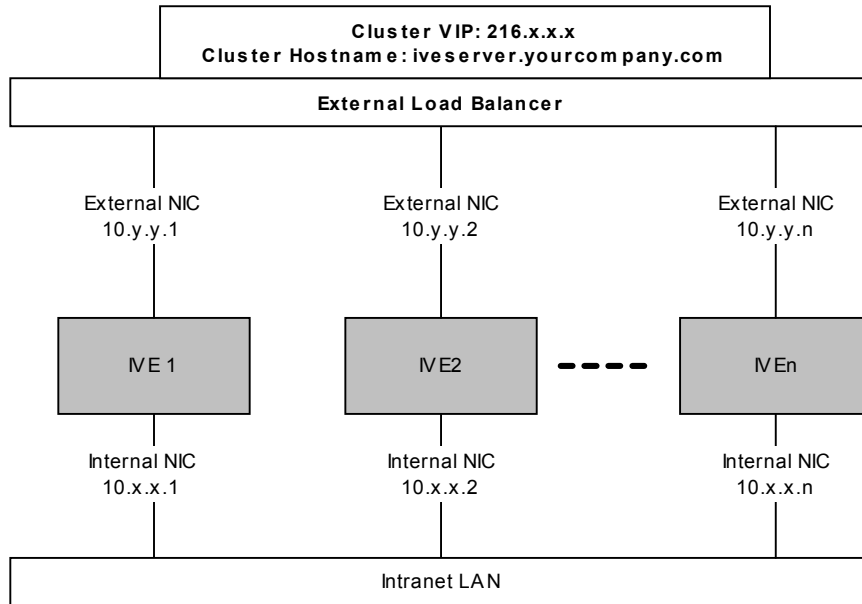
`https://<IVE-Hostname>/dana-na/healthcheck/healthcheck.cgi`

---

**Hinweis:** In der vorherigen Version wurden nur standardmäßige L3/L4-basierte Überprüfungen von einem externen Load-Balancer unterstützt.

---

**Abbildung 92** zeigt eine IVE-Clusterkonfiguration vom Typ Aktiv/Aktiv, bei der für die IVEs externe Ports aktiviert sind.

**Abbildung 92: Aktiv/Aktiv-Konfiguration**

Diese Abbildung zeigt eine Aktiv/Aktiv-Clusterkonfiguration, die hinter einem externen Load-Balancer bereitgestellt wird. Sie können ein Clusterpaar im Aktiv/Aktiv-Modus oder einen Multi-Unit-Cluster verwenden, der definitionsgemäß als Aktiv/Aktiv-Konfiguration ausgeführt wird. IVE-Benutzeranforderungen werden an die auf dem Load-Balancer definierte Cluster-VIP geleitet, der diese dann an das entsprechende IVE weiterleitet.

## Statussynchronisierung

Die IVE-Statussynchronisierung erfolgt nur über die internen NICs, und jedes Clustermitglied muss das Clusterkennwort besitzen, um mit anderen Mitgliedern kommunizieren zu können. Die Clustermitglieder synchronisieren Daten, wenn bei einem der Mitglieder des Clusters eine Statusänderung erfolgt. IVE-Clusterstatusdaten sind entweder **permanent**, d. h. permanent im IVE gespeichert, oder **vorübergehend**, d. h. nur für die Benutzersitzung im IVE gespeichert. IVE-Statusdaten werden in die folgenden Hauptkategorien unterteilt:

- **Systemstatus**—Dieser Status ist permanent und ändert sich nicht häufig.
  - Netzwerkeinstellungen
  - Authentifizierungsserver-Konfiguration
  - Konfiguration von Autorisierungsgruppen, zum Beispiel Zugriffssteu-  
rungsliste, Lesezeichen, Nachrichtenübermittlung und Anwendungsdaten
- **Benutzerprofil**—Diese Daten können permanent oder vorübergehend sein, je nachdem, ob beständige Cookies (Seite 149) und permanente Kennwortzwi-  
schenspeicherung (Seite 135) aktiviert sind. Wenn keine dieser Funktionen aktiviert ist, sind die Daten vorübergehend und fallen in die nächste Kategorie.
  - Benutzerlesezeichen—permanent
  - Permanente Benutzercookies—Wenn die Funktion für permanente  
Cookies aktiviert ist, speichert das IVE Benutzercookies für Websites,  
die permanente Cookies ausgeben.
  - Permanente Benutzerkennwörter—Wenn die Funktion zum Zwischenspei-  
chern von Kennwörtern aktiviert ist, können Benutzer festlegen, dass  
ihre Anmeldeinformationen für Anwendungen und Websites gespeichert  
werden.
- **Benutzersitzung**—Dieser Status ist vorübergehend und dynamisch. Die  
Benutzersitzungsdaten umfassen Folgendes:
  - Das IVE-Sitzungscookie des Benutzers
  - Vorübergehende Benutzerprofildaten, zu denen Cookies und Kennwörter  
zählen, die nur während der Benutzersitzung gespeichert werden.
- **Überwachungstatus**—Dieser permanente Status ist dynamisch und besteht  
aus Protokollmeldungen.<sup>1</sup>

---

1. Wenn Sie ein IVE zu einem Cluster hinzufügen, sendet der Clusterleiter keine Protokollmeldungen an das neue Mitglied. Protokollmeldungen werden nicht zwischen Clustermitgliedern synchronisiert, wenn ein Mitglied seinen Dienst wieder aufnimmt oder ein offline geschaltetes IVE wieder online geschaltet wird. Sobald alles IVEs online sind, werden die Protokollmeldungen jedoch synchronisiert.



Das IVE ist für die Synchronisation von Daten zwischen Clustermitgliedern verantwortlich, unabhängig davon, ob Sie einen Cluster im Aktiv/Passiv-Modus oder im Aktiv/Aktiv-Modus bereitstellen. Das IVE synchronisiert alle Systemdaten, Benutzerprofildaten und das IVE-Benutzersitzungscookie sofort. Wenn ein Clustermitglied offline geschaltet wird, müssen sich die Benutzer daher nicht erneut am IVE anmelden. Wenn das IVE Benutzersitzungsprofile synchronisiert und Statusdaten überwacht, tritt eine geringfügige Latenz auf. Falls ein Mitglied offline geschaltet wird, kann es passieren, dass sich der Benutzer bei manchen Back-End-Webanwendungen anmelden muss und Administratoren keinen Zugriff auf die Protokolle auf dem ausgefallenen Computer haben.

Die Synchronisationseinstellungen können auf zwei Arten konfiguriert werden:

- **Festlegen des Synchronisationsprotokolls**

Sie können das Synchronisationsprotokoll wählen, das der Konfiguration Ihrer Netzwerkhardware am besten entspricht:

- **Unicast**

Das IVE sendet die gleiche Meldung an jeden Knoten im Cluster.

- **Multicast**

Das IVE sendet eine Meldung an alle Clusterknoten im Netzwerk.

- **Broadcast**

Das IVE sendet eine Meldung an alle Geräte im Netzwerk, wobei nicht zum Cluster gehörige Knoten die Meldung löschen.

- **Festlegen, ob Protokollmeldungen synchronisiert werden sollen**

Protokollmeldungen können zu umfangreicher Belastung des Netzwerks führen und die Clusterleistung beeinträchtigen. Wir empfehlen, diese Option zu deaktivieren, insbesondere bei einer Multi-Unit-Konfiguration.

---

## Konfigurieren des IVE als Webproxy

Sie können alle vom IVE durchgeführten Webanforderungen an einen Webproxy leiten, statt mit dem IVE direkt eine Verbindung mit den Webservern herzustellen. Diese Funktion bietet sich an, wenn Ihre Richtlinien für die Netzwerksicherheit diese Konfiguration erfordern oder wenn Sie zur Leistungssteigerung einen Webproxy mit Zwischenspeicherung verwenden möchten.

Gegenwärtig gilt Folgendes:

- Das IVE unterstützt nur HTTP-Proxys; Secure-HTTP (HTTPS)-Proxys werden nicht unterstützt. Das IVE ruft Secure-HTTP-Inhalte über eine direkte Verbindung ab.

- Das IVE unterstützt keine Authentifizierung über Webproxys. Wenn Sie die Webproxy-Funktion des IVE verwenden möchten, müssen Sie Ihren Webproxy so konfigurieren, dass nicht authentifizierte Benutzer akzeptiert werden.

Schrittweise Anleitungen zum Konfigurieren des IVE für die Weiterleitung von Webanforderungen an einen Webproxy finden Sie auf Seite 264.

---

## Konfigurieren der Aktualisierungsoption für Secure Email Client

Die vom IVE bereitgestellte E-Mail-Unterstützung hängt von den optionalen Funktionen ab, die für den IVE-Server lizenziert sind:

- **Aktualisierungsoption für den Secure Email Client**

Wenn Ihre IVE-Lizenz die Aktualisierungsoption für den Secure Email Client umfasst, unterstützt das IVE IMAP4 (Internet Mail Application Protocol), POP3 (Post Office Protocol) und SMTP (Simple Mail Transfer Protocol). Sie können problemlos auf firmeninterne IMAP/POP/SMTP-Mailserver zugreifen, indem Sie im Menü **Email Settings** (Seite 267) den Mailserver, die E-Mail-Sitzung und die Authentifizierungsdaten angeben.

- **Aktualisierungsoption für Secure Application Manager**

Wenn Ihre IVE-Lizenz die Aktualisierungsoption für Secure Application Manager umfasst, unterstützt das IVE das systemeigene MAPI-Protokoll von Microsoft Exchange und das systemeigene Lotus Notes-Protokoll. Sie können den Zugriff auf Microsoft Exchange Server und Lotus Notes Server auf der Registerkarte **Applications** einer Autorisierungsgruppe aktivieren.

---

**Wichtig:** Wenn der IVE-Server mit der Secure Application Manager-Upgradeoption lizenziert ist, die das systemeigene MAPI-Protokoll von Microsoft Exchange und das systemeigene Lotus Notes-Protokoll unterstützt, trifft dieser Abschnitt nicht zu. Weitere Informationen finden Sie unter „Applications > Unterregisterkarte „Secure Application Manager (J-SAM)““ auf Seite 193.

---

Die Secure Email Client-Upgradeoption bietet Benutzern die Möglichkeit, mit standardbasierten E-Mail-Clients sicher von Remotestandorten aus auf firmeninterne E-Mail-Nachrichten zuzugreifen, ohne dass weitere Software, wie zum Beispiel ein VPN-Client, benötigt wird. Der Neoteris IVE-Server kann mit jedem Mailserver eingesetzt werden, der IMAP4 (Internet Mail Application Protocol), POP3 (Post Office Protocol) und SMTP (Simple Mail Transfer Protocol) unterstützt. Hierzu zählen auch Microsoft Exchange Server und Lotus Notes Mail Server, die IMAP4/POP3/SMTP-Schnittstellen zur Verfügung stellen.

Der Neoteris IVE-Server befindet sich zwischen dem Remoteclient und dem Mailserver und fungiert als sicherer E-Mail-Proxy. Der Remoteclient verwendet den Neoteris IVE-Server als (virtuellen) Mailserver und sendet E-Mail-Nachrichten über das SSL-Protokoll. Der Neoteris IVE-Server beendet SSL-Verbindungen des Clients und leitet den entschlüsselten E-Mail-Verkehr innerhalb des LAN an den Mailserver weiter. Der Neoteris-Server wandelt den unverschlüsselten Datenverkehr des Mailservers dann in S-IMAP (Secure IMAP)-, S-POP (Secure POP)- und S-SMTP (Secure SMTP)-Datenverkehr um und sendet ihn über SSL an den E-Mail-Client.

## Auswählen eines E-Mail-Clients

Das Neoteris IVE unterstützt die folgenden E-Mail-Clients:

- Outlook 2000 und 2002
- Outlook Express 5.5 und 6.x
- Netscape Messenger 4.7x und Netscape Mail 6.2

Benutzer, die Remotezugriff auf E-Mail-Nachrichten benötigen, können normalerweise in zwei Kategorien eingeteilt werden:

- **Laptopbenutzer in der Firma**

Diese Benutzer verwenden im Büro und unterwegs das gleiche Laptop.

- **Benutzer mit Heimcomputern**

Diese Benutzer verwenden zu Hause einen anderen Computer als im Büro.

Bevor Sie Benutzern einen E-Mail-Client empfehlen, sollten Sie die folgenden Abschnitte lesen, in denen erläutert wird, wie die unterstützten Clients mit folgenden Komponenten interagieren:

- Standardbasierte Mailserver (236)
- Microsoft Exchange Server (236)
- Lotus Notes und Lotus Notes Mail Server (239)

---

**Hinweis:** Anleitungen zum Konfigurieren der unterstützten E-Mail-Clients finden Sie auf der Neoteris Support-Site unter folgender Adresse: <http://support.neoteris.com>.

---

## Arbeiten mit einem standardbasierten Mailserver

Der Neoteris IVE-Server kann zusammen mit Mailservern verwendet werden, die IMAP4, POP3 und SMTP unterstützen.

### IMAP-Mailserver

- **Laptopbenutzer in der Firma:** Diese Benutzer können jeden der sechs unterstützen E-Mail-Clients verwenden. Wir empfehlen, im Büro und unterwegs den gleichen Client zu verwenden, um übergangsloses Arbeiten zu ermöglichen. Der Client muss dabei so konfiguriert sein, dass er auf den Neoteris IVE-Server verweist.
- **Benutzer mit Heimcomputern:** Diese Benutzer können für den Remotezugriff auf den IMAP-Server über das Neoteris IVE jeden der sechs unterstützten E-Mail-Clients verwenden.

### POP-Mailserver

- **Laptopbenutzer in der Firma:** Diese Benutzer können einen der vier Outlook-E-Mail-Clients\* verwenden. Wir empfehlen, im Büro und unterwegs den gleichen Client zu verwenden, um übergangsloses Arbeiten zu ermöglichen. Der Client muss dabei so konfiguriert sein, dass er auf den Neoteris IVE-Server verweist.
- **Benutzer mit Heimcomputern:** Diese Benutzer können für den Remotezugriff auf den POP-Server über das Neoteris IVE einen der vier Outlook-E-Mail-Clients\* verwenden.

\*Die Netscape-E-Mail-Clients können nicht im POP-Modus für den Remotezugriff verwendet werden, da sie S-POP nicht unterstützen. Dieses Protokoll wird jedoch vom Neoteris IVE-Server für die sichere Datenübertragung gefordert.

## Arbeiten mit Microsoft Exchange Server

Microsoft Exchange Server unterstützt:

- Systemeigene MAPI-Clients (Messaging Application Programming Interface)
- IMAP-Clients
- POP-Clients
- Outlook Web Access (OWA)

Der Neoteris IVE-Server bietet Zugriff auf Microsoft Exchange Server über IMAP- und POP-Clients unter Verwendung der Aktualisierungsoption für den

Secure Email Client und über OWA mit der Funktion für die sicheres Webbrowsing.

Wenn Sie den Zugriff auf Microsoft Exchange Server über das systemeigene MAPI-Protokoll ermöglichen möchten, muss das IVE mit den Aktualisierungsoption für Secure Application Manager lizenziert sein.

## Exchange Server und IMAP-Clients

Falls es sich bei dem firmeneigenen Mailserver um Exchange Server handelt, ist der Bürocomputer eines Mitarbeiters wahrscheinlich für die Verwendung des E-Mail-Clients Outlook 2000 oder 2002 im systemeigenen MAPI-Modus konfiguriert.

- Laptopbenutzer in der Firma: Diese Benutzer können einen der Outlook Express- oder Netscape-Clients für den Remotezugriff auf Exchange Server über das Neoteris IVE verwenden.<sup>1</sup>
- Benutzer mit Heimcomputern: Diese Benutzer können einen der sechs unterstützten E-Mail-Clients für den Remotezugriff auf Exchange Server über das Neoteris IVE verwenden, wobei davon ausgegangen wird, dass auf dem Remotecomputer kein MAPI-Konto konfiguriert ist.

Wenn Benutzer die Outlook Express- oder Netscape-Clients im IMAP-Modus ausführen, beachten Sie bitte das folgende Verhalten bei der Ordnerverwaltung:

- Bei Verwendung von Outlook Express-E-Mail-Clients  
Gelöschte E-Mail-Nachrichten werden im Posteingang von Outlook Express durchgestrichen angezeigt. Sie werden nicht in den Ordner Gelöschte Objekte auf dem Exchange Server verschoben, was bei Verwendung des Outlook 2000- oder 2002-Clients der Fall ist. Wenn ein Benutzer gelöschte E-Mail-Nachrichten in einem Outlook Express-Client entfernt, werden die E-Mail-Nachrichten endgültig gelöscht. Wir empfehlen Benutzern von Outlook Express die folgende Vorgehensweise:
  - Zu löschende E-Mail-Nachrichten sollten manuell in den unter Lokale Ordner angeordneten Ordner **Gelöschte Objekte** verschoben werden (hierbei handelt es sich um Standardordner). Dieser Ordner wird mit dem Ordner Gelöschte Objekte auf dem Exchange Server synchronisiert, wodurch Benutzer die Möglichkeit erhalten, gelöschte E-Mail-Nachrichten später abzurufen.

---

1. Der Outlook 2000-Client unterstützt nur eine Mailserverkonfiguration, in diesem Fall den systemeigenen MAPI-Modus. Dies verhindert, dass Benutzer den gleichen Client für den Remotezugriff verwenden. Der Outlook 2002-Client bietet Unterstützung für gleichzeitige MAPI- und IMAP-Serverkonfigurationen. Er unterstützt jedoch den IMAP-Zugriff nicht, wenn das MAPI-Konto offline ist, und verhindert hierdurch, dass Remotebenutzer E-Mail-Nachrichten abrufen können.

- Sie sollten die gelöschten E-Mail-Nachrichten zunächst im Posteingang von Outlook Express lassen und dann bei der nächsten Anmeldung bei Outlook 2000 oder 2002 die gelöschten E-Mail-Nachrichten in den Ordner Gelöschte Objekte verschieben.
- Bei Verwendung von Netscape-E-Mail-Clients  
Gelöschte E-Mail-Nachrichten werden in den Papierkorbordner von Netscape verschoben und im Posteingang von Netscape nicht mehr angezeigt. Aus dem Posteingang von Outlook 2000 oder 2002 werden sie jedoch erst dann entfernt, wenn die Benutzer folgendermaßen vorgehen:
  - 1 Sie sollten Netscape so konfigurieren, dass gelöschte Nachrichten in den Papierkorbordner verschoben werden, und die Option zum Leeren des Posteingangs bei Beendigung des Programms aktivieren.
  - 2 Sie sollten immer nur eines der Programme ausführen und schließen, wenn Sie Ihre Arbeit beendet haben. Der Posteingang des anderen Programms wird dann mit dem Server synchronisiert, sodass die gleichen Nachrichten angezeigt werden.

Gesendete E-Mail-Nachrichten werden außerdem in den Netscape-Ordner für gesendete Objekte (oder einen anderen benutzerdefinierten Ordner) verschoben. Wenn Benutzer möchten, dass gesendete Nachrichten im Ordner Gesendete Objekte von Microsoft Exchange Server angezeigt werden, müssen sie sie manuell aus dem Netscape-Ordner für gesendete Objekte in den Ordner Gesendete Objekte ziehen.

## Exchange Server und POP-Clients

Falls es sich bei dem firmeneigenen Mailserver um Exchange Server handelt, ist der Bürocomputer eines Mitarbeiters wahrscheinlich für die Verwendung des E-Mail-Clients Outlook 2000 oder 2002 im systemeigenen MAPI-Modus konfiguriert.

- Laptopbenutzer in der Firma: Diese Benutzer können für den Remotezugriff auf Exchange Server über das Neoteris IVE einen der unterstützten Outlook Express-Clients\* verwenden.
- Benutzer mit Heimcomputern: Diese Benutzer können für den Remotezugriff auf Exchange Server über das Neoteris IVE einen der vier Outlook-Clients\* verwenden, wobei davon ausgegangen wird, dass auf dem Remotecomputer kein MAPI-Konto konfiguriert ist.

\*Die Netscape-E-Mail-Clients können nicht im POP-Modus für den Remotezugriff verwendet werden, da sie S-POP nicht unterstützen. Dieses Protokoll wird jedoch vom Neoteris IVE-Server für die sichere Datenübertragung gefordert.

## Exchange Server und Outlook Web Access

Um auf dem Exchange-Server OWA-Zugriff zur Verfügung zu stellen und es Benutzern zu ermöglichen, über die Webbrowsingfunktion von Neoteris IVE auf den Exchange-Server zuzugreifen, müssen Sie lediglich OWA im Intranet als webbasierte Anwendung bereitstellen. Es ist keine weitere Einrichtung erforderlich, um eine OWA-Implementierung außerhalb des Netzwerks bereitzustellen.

---

**Hinweis:** Bei Verwendung des Neoteris IVE-Servers für den Zugriff auf Outlook Web Access wird der IIS-Webserver für OWA vor Standardangriffen (z. B. Nimda) geschützt und bietet daher erheblich höhere Sicherheit als der Einsatz von OWA direkt über das Internet.

---

## Arbeiten mit Lotus Notes und Lotus Notes Mail Server

Lotus Notes Mail Server stellt POP3- und IMAP4-Schnittstellen zur Verfügung und ermöglicht Benutzern somit das Abrufen von E-Mail-Nachrichten von einer Lotus Notes-E-Mail-Konfiguration über das Neoteris IVE. Um zu ermitteln, welcher E-Mail-Client sich für die E-Mail-Benutzer im Unternehmen empfiehlt, die Remotezugriff auf den Lotus-Mailserver benötigen, lesen Sie bitte den Abschnitt über das Arbeiten mit standardbasierten Mailservern auf Seite 236.

---

## Überwachen des IVE als SNMP-Agent

Mit einem Netzwerkverwaltungstool wie HP OpenView können Sie das IVE als SNMP-Agent überwachen. Das IVE unterstützt SNMP v2, implementiert eine private MIB (Management Information Base) und definiert eigene Traps. Um die Verarbeitung dieser Traps in der Netzwerkverwaltungsstation zu ermöglichen, müssen Sie die Neoteris-MIB-Datei herunterladen und die entsprechenden Angaben zum Empfangen der Traps machen.

---

**Hinweis:** Zum Überwachen wesentlicher IVE-Systemstatistiken, beispielsweise der CPU-Auslastung, laden Sie die UC-Davis-MIB-Datei in Ihre SNMP-Managementanwendung. Sie erhalten die MIB-Datei im Internet unter folgender Adresse:  
<http://net-snmp.sourceforge.net/UCD-SNMP-MIB.txt>

---

## Network > Menü „Network Settings“

Im Menü **Network > Network Settings** können Sie folgende Aufgaben durchführen:

- Ändern von Netzwerkeinstellungen für den internen Port (LAN-Schnittstelle) (240)
- Aktivieren des externen Ports (DMZ-Schnittstelle) (241)
- Angeben von statischen Routen für den Netzwerkverkehr (243)

Übersichtsinformationen zu Netzwerkeinstellungen finden Sie unter „Konfigurieren allgemeiner Netzwerkeinstellungen für das IVE“ auf Seite 226.

## Registerkarte „Internal Port“

### ☒ Ändern von Netzwerkeinstellungen für den internen Port (LAN-Schnittstelle)

Auf der Registerkarte **Internal Port** können Sie die Netzwerkeinstellungen ändern, die Sie während der Ersteinrichtung angegeben haben. Weitere Informationen zu allgemeinen Netzwerkeinstellungen finden Sie auf Seite 226.

#### So ändern Sie die Netzwerkeinstellungen für den internen Port

1. Wählen Sie in der Administratorkonsole die Registerkarte **Network > Network Settings > Internal Port** aus.
2. Geben Sie die neuen Informationen ein, und klicken Sie dann auf **Save Changes**.

---

**Hinweis:** Um auf die letzten gespeicherten Änderungen zurückzusetzen, klicken Sie auf **Reset**.

---



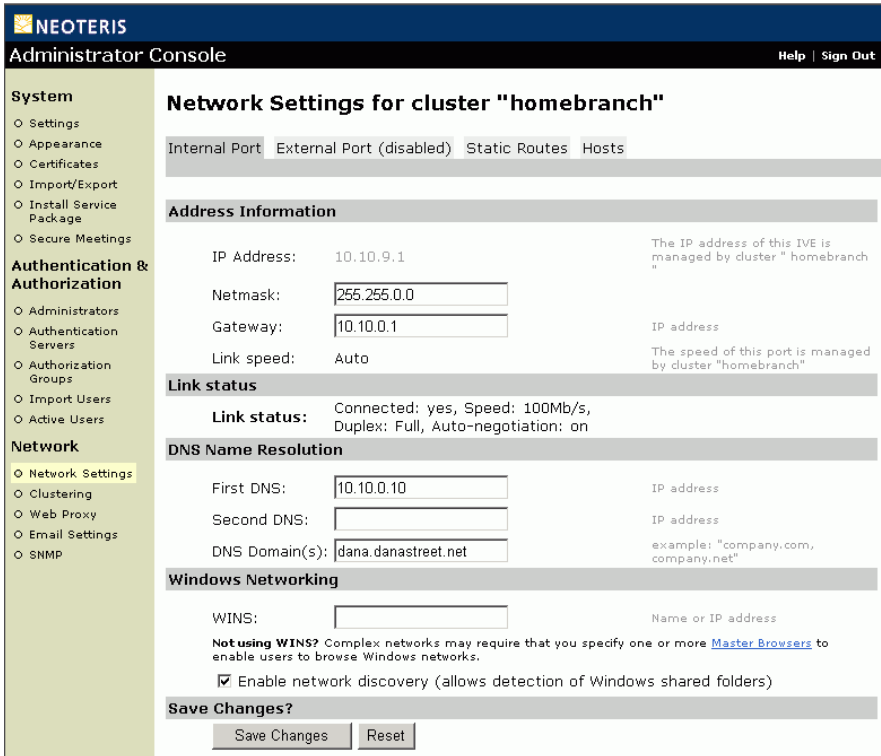


Abbildung 93: Network > Network Settings > Internal Port

## Registerkarte „External Port“

### ☒ Aktivieren des externen Ports (DMZ-Schnittstelle)

Auf der Registerkarte **External Port** können Sie die DMZ-Funktion aktivieren. Weitere Informationen zu allgemeinen Netzwerkeinstellungen finden Sie auf Seite 226.

---

**Hinweis:** Der externe Port fragt nur Anforderungen von Benutzern ab, die am IVE angemeldet sind, und leitet nur deren Anforderungen weiter. Wenn Sie die DMZ-Funktion aktivieren, können sich Administratoren standardmäßig nicht mehr von einem externen Standort aus anmelden. Sie können den externen Port für Administratoren auf der Registerkarte **Authentication & Authorization > Administrators > Authentication > Address Restrictions** öffnen.

---

## So aktivieren Sie den externen Port

1. Wählen Sie in der Administratorkonsole die Registerkarte **Network** > **Network Settings** > **External Port** aus.
2. Wählen Sie unter **DMZ Setting** die Option **Enable** aus.
3. Geben Sie unter **Address Information** die IP-Adresse, die Netzmaske und die Gateway-Informationen für den externen Port des IVE ein. In den meisten Fällen empfiehlt es sich, die Einstellungen von der Seite **Internal Port** zu übernehmen und dann die Informationen zum internen Port in eine lokale IP-Adresse und Netzmaske sowie ein lokales Gateway zu ändern.
4. Klicken Sie zum Speichern der Einstellungen auf **Save Changes**.

**NEOTERIS**  
Administrator Console Help | Sign Out

**System**

- Settings
- Appearance
- Certificates
- Import/Export
- Install Service Package
- Secure Meetings

**Authentication & Authorization**

- Administrators
- Authentication Servers
- Authorization Groups
- Import Users
- Active Users

**Network**

- Network Settings
- Clustering
- Web Proxy
- Email Settings
- SNMP

### Network Settings for cluster "homebranch"

Internal Port External Port (disabled) Static Routes Hosts

The external port can be used to enable more secure configurations.

**DMZ Setting**

☐ Enable ☒ Disable

**Address Information**

IP Address: 10.8.9.1 The external IP address of this IVE is managed by cluster "homebranch"

Netmask:

Gateway:  IP address

Link speed: Auto The speed of this port is managed by cluster "homebranch"

Note: If you need to specify static routes, you can do so on the [Static Routes](#) page.

**Link status**

**Link status:** Connected: no, Speed: 10Mb/s, Duplex: Half, Auto-negotiation: on

**Save Changes?**

Abbildung 94: Network > Network Settings > External Port

**Hinweis:** Wenn der IVE-Server nicht mit der optionalen DMZ-Funktion lizenziert ist, werden auf der Seite **Network Settings** nur die Registerkarten **Network Port** und **Static Routes** angezeigt.

## Registerkarte „Static Routes“

### ☒ Angeben von statischen Routen für den Netzwerkverkehr

Auf der Registerkarte **Static Routes** können Sie Routingtabelleneinträge hinzufügen. Weitere Informationen zu allgemeinen Netzwerkeinstellungen finden Sie auf Seite 226.

---

**Hinweis:** Alle Verbindungsanforderungen an interne Ressourcen erfolgen von dem internen IVE-Port aus, unabhängig von den Routeneinstellungen. Die Routeneinstellungen des externen Ports werden nur zur Weiterleitung von Paketen verwendet, die Verbindungen zugeordnet sind, die von einem Remoteclient initiiert wurden.

---

### So geben Sie statische Routen an

1. Wählen Sie in der Administratorkonsole die Registerkarte **Network > Network Settings > Static Routes** aus.
2. Geben Sie die erforderlichen Informationen ein, und klicken Sie auf **Add**.

NEOTERIS

Administrator Console

Help | Sign Out

System

- Settings
- Appearance
- Certificates
- Import/Export
- Install Service Package
- Secure Meetings

Authentication & Authorization

- Administrators
- Authentication Servers
- Authorization Groups
- Import Users
- Active Users

Network

- Network Settings
- Clustering
- Web Proxy
- Email Settings
- SNMP

Network Settings for cluster "homebranch"

Internal Port

External Port (disabled)

Static Routes

Hosts

Many typical networks will not require changes to these routing tables, but if you need to add additional routes, you can do so here.

These are the routing table entries that are *common* for the nodes in the cluster. Individual nodes may have extra routing table entries.

Network Routing Table

Destination	Netmask	Gateway	Metric (0-15)	
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	Add
default	0.0.0.0	10.10.0.1	0	Default

Abbildung 95: Network > Network Settings > Static Routes

## Registerkarte „Hosts“

### ☒ **Angeben von Hostnamen, die vom IVE lokal aufgelöst werden sollen**

Auf der Registerkarte **Hosts** können Sie Hostnamen angeben, die vom IVE lokal zu IP-Adressen aufgelöst werden können. Diese Funktion bietet sich in folgenden Fällen an:

- Das IVE kann nicht auf den DNS-Server zugreifen
- Im LAN wird über WINS auf Server zugegriffen
- Die Sicherheitsrichtlinien Ihres Unternehmens lassen die Auflistung interner Server auf einem externen DNS nicht zu oder erfordern die Maskierung interner Hostnamen

Wenn Sie auf der Registerkarte **Network Settings > Hosts** eines Clusters Zuordnungen von Hostnamen eingeben, werden die Einstellungen von den anderen Knoten übernommen. Wenn Sie Zuordnungen von Hostnamen für einen bestimmten Knoten eingeben möchten, wählen Sie das Menü **Clustering** aus, wählen dann in der Liste **Cluster Members** einen Knoten aus und wählen für diesen Knoten dann die Registerkarte **Hosts** aus.

### **So geben Sie Hostnamen an, die das IVE lokal auflösen soll**

1. Wählen Sie in der Administratorkonsole die Registerkarte **Network > Network Settings > Hosts** aus.
2. Geben Sie eine IP-Adresse, eine durch Kommas getrennte Liste von Hostnamen, die zu der IP-Adresse aufgelöst werden, und bei Bedarf einen Kommentar von höchstens 200 Wörtern ein, und klicken Sie dann auf **Add**.

NEOTERIS

Administrator Console

Help | Sign Out

System

- Settings
- Appearance
- Certificates
- Import/Export
- Install Service Package
- Secure Meetings

Authentication & Authorization

- Administrators
- Authentication Servers
- Authorization Groups
- Import Users
- Active Users

Network

- Network Settings
- Clustering
- Web Proxy
- Email Settings

Network Settings for cluster "homebranch"

Internal Port

External Port (disabled)

Static Routes

Hosts

To allow the IVE to resolve specific hostnames to IP addresses without relying on DNS, create IP address/hostname mappings below. Cluster nodes share these mappings. Individual nodes may have additional mappings.

Hosts:

IP	Name	Comment	
<input type="text"/>	<input type="text"/>	<input type="text"/>	Add

Abbildung 96: Network > Network Settings > Hosts

## Network > Menü „Clustering“

In diesem Abschnitt werden Verwaltungsaufgaben erläutert, die sich auf das Erstellen und Verwalten eines Clusterpaars beziehen. Im Einzelnen sind dies folgende Aufgaben:

Definieren und Initialisieren eines Clusters .....	247
Hinzufügen eines IVEs zu einem Cluster über die serielle Konsole .....	249
Hinzufügen eines IVEs zu einem Cluster über die Administratorkonsole .....	254
Aktualisieren eines Clusters .....	256
Verwalten von Clusterknoten und Angeben neuer Clustermitglieder .....	257
Ändern von Clustereigenschaften oder Löschen eines Clusters .....	262

Übersichtsinformationen zu Clustern finden Sie unter „Konfigurieren eines Clusters von IVE-Servern“ auf Seite 227.

Wir empfehlen, einen Cluster zunächst in einer Stagingumgebung bereitzustellen und erst zu einer Produktionsumgebung zu wechseln, nachdem Sie den Autorisierungsserver und die Konfiguration der Autorisierungsgruppen sowie die Anwendungen, die die Endbenutzer möglicherweise verwenden, getestet haben.

---

**Wichtig:** Vor dem Erstellen eines Clusters müssen Sie sicherstellen, dass es sich bei allen vorgesehenen IVE-Knoten um den gleichen Typ von Neoteris-Hardware handelt und dass auf allen Knoten die gleiche Dienstpaketversion ausgeführt wird.

---

### ☒ Definieren und Initialisieren eines Clusters

Beim Erstellen eines Clusterpaares oder eines Multi-Unit-Clusters werden zunächst die Clustereinstellungen für ein IVE festgelegt, und anschließend werden weitere Mitglieder zu dem Cluster hinzugefügt. Wir empfehlen, vor dem Definieren eines Clusters zunächst die System-, Authentifizierungs-, Autorisierungs- und Netzwerkeinstellungen auf einem IVE zu definieren. Definieren Sie anschließend auf dem gleichen IVE den Cluster. Dieses IVE wird dem Cluster im Rahmen des Erstellungsvorgangs hinzugefügt.

## So definieren und initialisieren Sie einen Cluster

1. Konfigurieren Sie ein IVE mit den gewünschten System-, Authentifizierungs-, Autorisierungs- und Netzwerkeinstellungen.
2. Wählen Sie in der Administratorkonsole des konfigurierten IVEs die Registerkarte **System > Settings > License** aus, und geben Sie Ihren Lizenzcode ein, um die Clusterfunktion zu aktivieren. Die Menüoption **Clustering** wird unter der Überschrift **Network** angezeigt.
3. Geben Sie auf der Seite **Network > Clustering** unter **Clustering** die Bezeichnung für den Cluster, ein Clusterkennwort und einen Namen für dieses Gerät ein, zum Beispiel **ive-1**.

**Hinweis:** Wenn Sie weitere IVEs konfigurieren, die dem Cluster hinzugefügt werden sollen, müssen Sie das Kennwort erneut eingeben. Alle IVEs in dem Cluster verwenden dieses Kennwort für die Kommunikation.

4. Klicken Sie auf **Create Cluster**. Nachdem das IVE den Cluster initialisiert hat, werden auf der Seite **Clustering** die Registerkarten **Status** und **Properties** angezeigt.

**NEOTERIS**  
Administrator Console Help | Sign Out

**System**

- Settings
- Appearance
- Certificates
- Import/Export
- Install Service Package

**Authentication & Authorization**

- Administrators
- Authentication Servers
- Authorization Groups
- Active Users

**Network**

- Network Settings
- **Clustering**
- Web Proxy
- Email Settings
- SNMP

**Clustering**

Type: Multi-Unit Cluster

Cluster Name:  Name of the cluster to create. Must be alphanumeric, "-", or "\_"

Cluster Password:

Confirm Password:

Member Name:  Name of this IVE in the cluster. Must be alphanumeric, "-", or "\_"

**Join existing cluster**

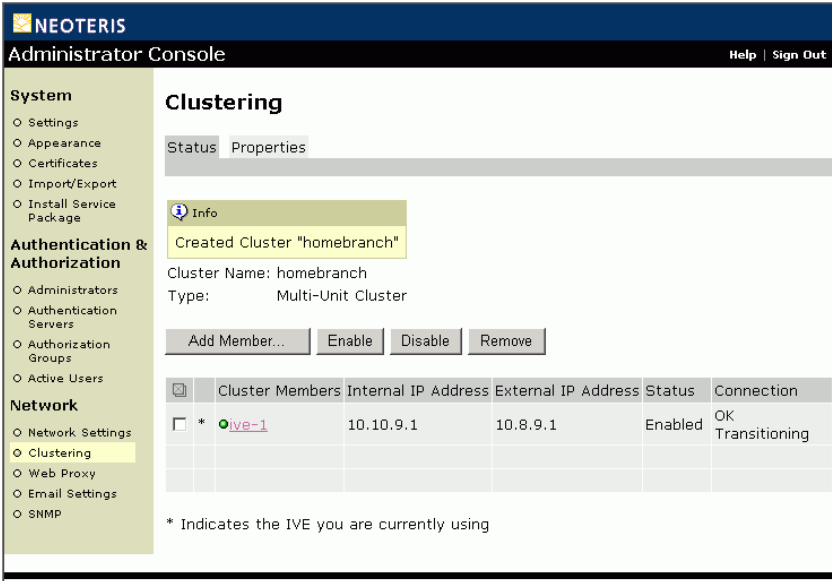
Cluster Name:  Name of the cluster to join

Cluster Password:

Existing Member Address:  IP address of any existing cluster member

Abbildung 97: Network > Clustering – Startseite





**Abbildung 98: Network > Clustering**  
Die Abbildung zeigt die Seite **Clustering** nach der Definition eines Clusters. Beachten Sie, dass das IVE, auf dem Sie den Cluster definieren, das erste Clustermitglied wird.

**☑ Hinzufügen eines IVEs zu einem Cluster über die serielle Konsole**

Sie können ein IVE über die serielle Konsole oder die Administratorkonsole zu einem Cluster hinzufügen. Wir empfehlen, die serielle Konsole zu verwenden, da bei diesem Verfahren nur wenige Informationen eingegeben müssen, um das IVE zum Cluster hinzuzufügen. Sobald der Cluster das hinzuzufügende IVE authentifiziert, erhält das neue Clustermitglied die Clusterstatuseinstellungen, die *alle* Einstellungen auf dem IVE überschreiben.

**Wichtig:** Wenn Sie ein IVE, das gegenwärtig als eigenständiges Gerät ausgeführt wird, über seine serielle Konsole zu einem Cluster hinzufügen möchten, muss das gleiche Softwarepaket auf der gleichen Hardwareplattform wie bei den anderen Mitgliedern ausgeführt werden.

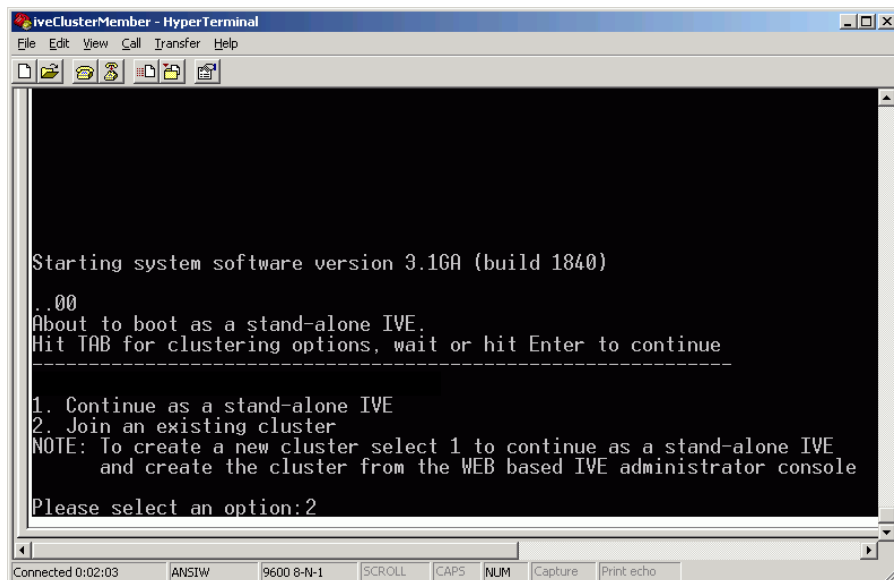
### So fügen Sie ein IVE über die serielle Konsole des Computers zu einem Cluster hinzu

1. Wählen Sie in der Administratorkonsole eines aktiven Clustermitglieds die Registerkarte **Network > Clustering > Status** aus, und geben Sie das IVE an, das dem Cluster hinzugefügt werden soll. Weitere Informationen finden Sie unter „So geben Sie ein IVE an, das einem bestehenden Cluster hinzugefügt werden soll“ auf Seite 258.
2. Stellen Sie eine Verbindung mit der seriellen Konsole des IVE her. Weitere Informationen finden Sie unter „Herstellen einer Verbindung mit der seriellen Konsole des IVE“ auf Seite 273.
3. Schalten Sie das IVE aus und dann wieder ein, und überwachen Sie beim Neustart die serielle Konsole. Nach dem Start der Systemsoftware werden Sie in einer Meldung darüber informiert, dass das Gerät als eigenständiges IVE gestartet wird und dass Sie die **TAB-Taste** drücken müssen, um die Clusteroptionen anzuzeigen. Drücken Sie die **TAB-Taste**, wenn Ihnen diese Meldung angezeigt wird.

---

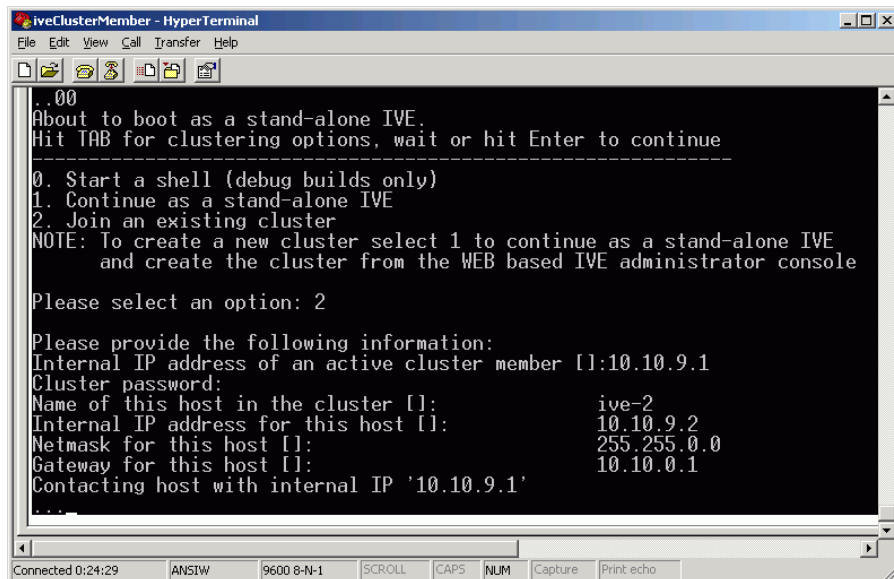
**Hinweis:** Sie müssen die **TAB-Taste** innerhalb von 5 Sekunden drücken. Wenn das Gerät bereits im eigenständigen Modus bootet, warten Sie, bis der Bootvorgang beendet ist, und starten Sie das Gerät dann neu.

---



**Abbildung 99: Serielle Konsole von Neoteris – Clusteroptionen**

4. Geben Sie die Nummer für den Beitritt zu dem bestehenden Cluster ein.
5. Geben Sie die erforderlichen Informationen ein. Dies sind:
  - Die interne IP-Adresse eines aktiven Clustermittglieds.
  - Das Clusterkennwort, d. h. das Kennwort, dass Sie beim Definieren des Clusters eingegeben haben.
  - Der Name des Geräts, das Sie hinzufügen möchten. In diesem Beispiel lautet der Name ive-2.
  - Die interne IP-Adresse des Geräts, das Sie hinzufügen möchten.
  - Die Netzmaske des Geräts, das Sie hinzufügen möchten.
  - Das Gateway des Geräts, das Sie hinzufügen möchten.



**Abbildung 100: Serielle Konsole von Neoteris: Angeben von Informationen zu dem neuen Clustermittglied**

Das von Ihnen angegebene aktive Clustermitglied überprüft das Clusterkennwort sowie den Namen und die IP-Adresse (oder Adresse) des Geräts, das Sie in der Administratorkonsole auf der Seite **Network > Clustering > Add Cluster Member** angegeben haben.

Wenn die Anmeldeinformationen gültig sind, wird eine Meldung mit einer Übersicht über die nächsten Schritte des Verfahrens angezeigt. Hierzu zählt das Kopieren sämtlicher Statusdaten von dem aktiven Mitglied auf das neue Clustermitglied einschließlich Lizenz und Zertifikat sowie aller übrigen Statusdaten.

```

iveClusterMember - HyperTerminal
File Edit View Call Transfer Help

-----
This host successfully contacted cluster member '10.10.9.1', and
received the following information about the cluster:
Cluster Name: homebranch
Cluster Members
  name| ip| netmask| gateway|enabled|
-----|-----|-----|-----|-----|
ive-1| 10.10.9.1| 255.255.0.0| 10.10.0.1| on|
*ive-2| 10.10.9.2| 255.255.0.0| 10.10.0.1| on|
-----|-----|-----|-----|-----|

This host is ready now to join the cluster as member 'ive-2'
WARNING: This host's entire state will be overwritten with the current
cluster configuration, including bookmarks, IP address, netmask etc.
Please select one of the options:

1. Continue join cluster operation
2. Abort and boot with the previous settings

Enter 1 or 2: 1
-----
Connected 0:48:58 ANSI 9600 8-N-1 SCROLL CAPS NUM Capture Print echo

```

**Abbildung 101: Serielle Konsole von Neoteris: Es wurde eine Verbindung mit dem aktiven Clustermitglied hergestellt**

6. Geben Sie zum Fortfahren die Nummer ein. Wenn die Meldung über die Bestätigung des Clusterbeitritts angezeigt wird, überprüfen Sie die Administratorkonsole jedes aktiven Clustermitglieds, um sicherzustellen, dass der Verbindungsstatus (**Connection**) auf **OK** gesetzt ist.

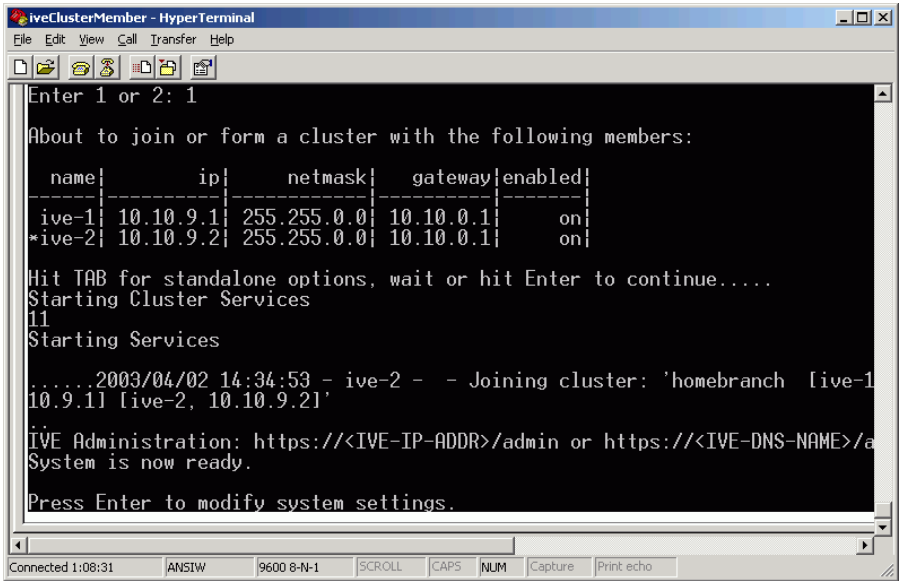


Abbildung 102: Serielle Konsole von Neoteris: Das neue Clustermitglied wurde erfolgreich hinzugefügt

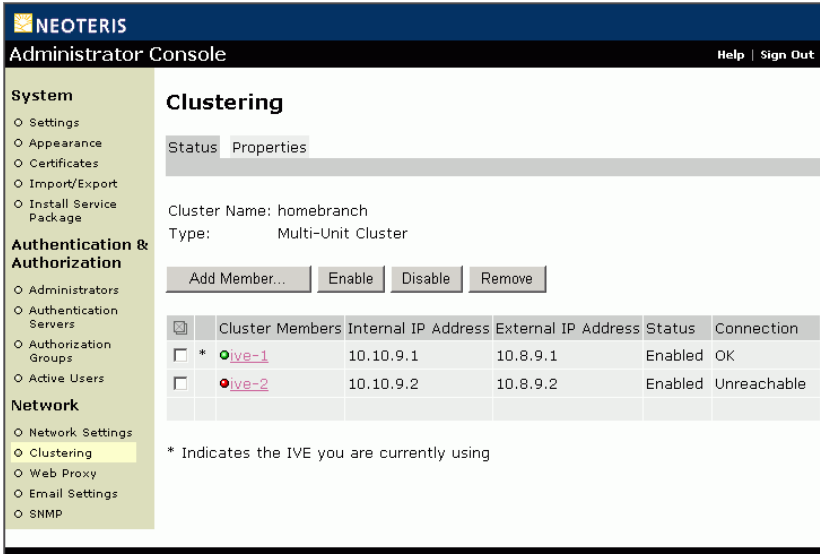


Abbildung 103: Network > Clustering > Status: Das neue Clustermitglied wurde erfolgreich hinzugefügt

## ☑ Hinzufügen eines IVEs zu einem Cluster über die Administratorkonsole

Ein nicht initialisiertes oder eigenständiges IVE kann entweder über die serielle Konsole oder über die Administratorkonsole zu einem Cluster hinzugefügt werden. Wir empfehlen, die serielle Konsole zu verwenden (siehe Seite 249), da bei diesem Verfahren nur wenige Informationen eingegeben müssen, um das IVE zum Cluster hinzuzufügen.

Falls Sie die Administratorkonsole bevorzugen und das IVE noch nicht initialisiert wurde, führen Sie die Ersteinrichtung des Geräts wie im Installationshandbuch beschrieben durch. Dieses Handbuch liegt dem Produkt bei und steht zudem auf der Website des Neoteris-Support im PDF-Format zur Verfügung.

---

**Wichtig:** Wenn Sie ein eigenständiges IVE über die Administratorkonsole zu einem Cluster hinzufügen möchten, muss dieses über die gleiche Lizenz verfügen wie die anderen Mitglieder. Außerdem muss das gleiche Softwarepaket auf der gleichen Hardwareplattform wie bei den anderen Mitgliedern ausgeführt werden.

---

### So fügen Sie ein IVE über die Administratorkonsole des IVEs zu einem Cluster hinzu

1. Wählen Sie in der Administratorkonsole eines aktiven Clustermitglieds die Registerkarte **Network > Clustering > Status** aus, und geben Sie das IVE an, das dem Cluster hinzugefügt werden soll. Weitere Informationen finden Sie unter „So geben Sie ein IVE an, das einem bestehenden Cluster hinzugefügt werden soll“ auf Seite 258.
2. Wählen Sie in der Administratorkonsole des IVEs, das Sie einem Cluster hinzufügen möchten, die Registerkarte **System > Settings > License** aus, und geben Sie Ihren Lizenzcode ein, um die Clusterfunktion zu aktivieren.
3. Geben Sie auf der Seite **Network > Clustering** unter **Join existing cluster** Folgendes ein:
  - Die Bezeichnung des Clusters, dem das IVE beitreten soll
  - Das Clusterkennwort, das Sie beim Definieren des Clusters angegeben haben
  - Die IP-Adresse eines aktiven Clustermitglieds
4. Klicken Sie auf **Join Cluster**.

NEOTERIS

Administrator Console

Help | Sign Out

System

- Settings
- Appearance
- Certificates
- Import/Export
- Install Service Package

Authentication & Authorization

- Administrators
- Authentication Servers
- Authorization Groups
- Active Users

Network

- Network Settings
- Clustering
- Web Proxy
- Email Settings
- SNMP

Clustering

Type:Multi-Unit Cluster

Cluster Name:Name of the cluster to create  
Must be alphanumeric, "-", or "\_"

Cluster Password:

Confirm Password:

Member Name:Name of this IVE in the cluster  
Must be alphanumeric, "-", or "\_"

Create Cluster

Join existing cluster

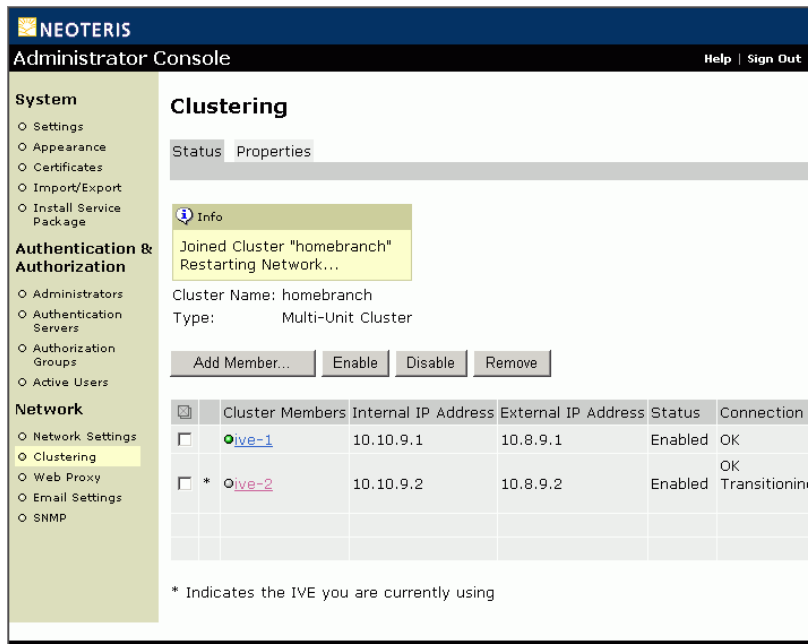
Cluster Name:homebranchName of the cluster to join

Cluster Password:\*\*\*\*\*

Existing Member Address:10.10.9.1IP address of any existing cluster member

Join Cluster

Abbildung 104: Network > Clustering: Beitreten zu einem Cluster



**Abbildung 105: Network > Clustering: Neustarten von Diensten auf einem neuen Clustermittglied**

Sobald ein neuer Knoten mit dem Cluster verbunden wird, wird der Clusterstatus auf der Registerkarte „Status“ des Clusters angezeigt.

## ☑ Aktualisieren eines Clusters

Zum Aktualisieren eines Clusters installieren Sie das gewünschte Dienstpaket auf jedem Clustermittglied. Wir empfehlen, einen Knoten vor dem Installieren eines Servicepakets zu deaktivieren.

**Hinweis:** Sie können Clustermittglieder nicht herunterstufen. Sie können jedes Clustermittglied jedoch durch ein Rollback auf seinen vorherigen Nicht-Cluster-Zustand zurücksetzen.

### So aktualisieren Sie einen Cluster

1. Melden Sie sich an der Administratorkonsole des Clusterknotens an, den Sie aktualisieren möchten. Um auf die Administratorkonsole eines Clusterknotens zuzugreifen, geben Sie in einem Browser seine interne IP-Adresse gefolgt von „/admin“ ein. Beispiel: <https://x.x.x.x/admin>



2. Aktivieren Sie auf der Registerkarte **Network > Clustering > Status** das Kontrollkästchen neben dem Namen des Knotens in der Spalte **Cluster Members**, und klicken Sie dann auf **Disable**.
3. Installieren Sie das Dienstpaket wie unter „Installieren eines Neoteris-Softwaredienstpakets“ auf Seite 66 beschrieben.
4. Nach Abschluss des Installationsvorgangs kehren Sie zur Registerkarte des Knotens **Network > Clustering > Status** zurück, aktivieren das Kontrollkästchen neben dem Namen des Knotens in der Spalte **Cluster Members** und klicken dann auf **Enable**.
5. Führen Sie diese Schritte für jeden Knoten im Cluster durch.

## Registerkarte „Status“

### ☒ Verwalten von Clusterknoten und Angeben neuer Clustermitglieder

Auf dieser Registerkarte können Sie den Status von Clusterknoten überwachen, die Netzwerkeinstellungen für einen bestimmten Knoten bearbeiten, IVEs angeben, die Sie einem Cluster hinzufügen möchten und Clusterknoten aktivieren, deaktivieren oder entfernen. In Tabelle 1 auf Seite 259 werden die auf der Registerkarte **Status** angezeigten Informationen sowie die verschiedenen durchführbaren Verwaltungsaufgaben erläutert.

#### So ändern Sie die Netzwerkeinstellungen eines Clusterknotens

1. Wählen Sie in der Administratorkonsole eines aktiven Clustermitglieds die Registerkarte **Network > Clustering > Status** aus.
2. Klicken Sie in der Spalte **Cluster Members** auf den Namen des Knotens, für den Sie Netzwerkeinstellungen ändern möchten.

Die Seite **Network Settings** mit den Registerkarten **Clustering**, **Internal Port**, **External Port** und **Static Routes** wird angezeigt. Wenn Sie Änderungen auf diesen Registerkarten speichern, wirken sich die neuen Einstellungen nur auf den entsprechenden Knoten aus.

---

**Wichtig:** Falls Sie die Netzwerkeinstellungen auf der Seite **Network > Network Settings** in der Administratorkonsole eines Clustermitglieds ändern, werden die Änderungen an jeden Knoten im Cluster weitergegeben. Um Einstellungen nur für einen bestimmten Knoten zu ändern, müssen Sie auf der Registerkarte „Status“ jedes aktiven Mitglieds eine Verknüpfung mit der Seite **Network Settings** des Knotens herstellen.

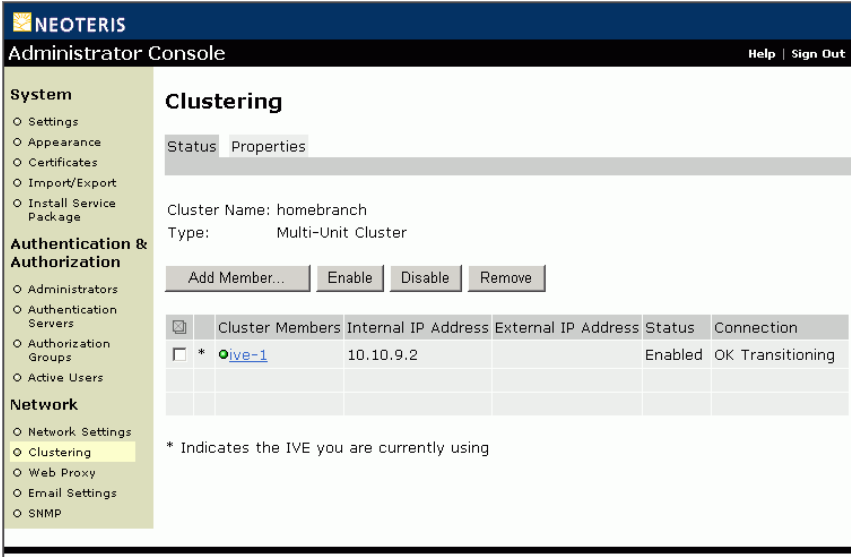
---

### So geben Sie ein IVE an, das einem bestehenden Cluster hinzugefügt werden soll

1. Wählen Sie in der Administratorkonsole eines aktiven Clustermitglieds die Registerkarte **Network > Clustering > Status** aus.
2. Klicken Sie auf **Add Member**, um ein IVE anzugeben, dass dem Cluster beiträgt:
  - 1 Geben Sie die Bezeichnung des Mitglieds ein.
  - 2 Geben Sie die interne IP-Adresse des Mitglieds ein.
  - 3 Geben Sie die externe IP-Adresse des IVE ein. Beachten Sie, dass das Feld **External IP address** nur angezeigt wird, wenn Sie den externen Port auf der Registerkarte **Network > Network Settings > External Port** aktiviert haben.
  - 4 Klicken Sie auf **Add Node**.
  - 5 Wiederholen Sie dieses Verfahren für jedes Gerät, das Sie hinzufügen möchten.

The screenshot shows the NEOTERIS Administrator Console interface. The left sidebar contains a navigation menu with categories: System, Authentication & Authorization, and Network. The 'Network' category is expanded, showing 'Network Settings', 'Clustering', 'Web Proxy', 'Email Settings', and 'SNMP'. The 'Clustering' option is selected, leading to the 'Add Cluster Member' form. The form includes fields for 'Cluster' (set to 'homebranch'), 'Member Name' (set to 'ive-2'), 'Internal IP address' (set to '10.10.9.2'), and 'External IP address' (set to '10.8.9.2'). A note indicates that characters must be alphanumeric, "-", or "\_". At the bottom of the form are 'Add Node' and 'Cancel' buttons.

Abbildung 106: Network > Clustering > Add Member



**Abbildung 107: Network > Clustering > Status**  
Die Abbildung zeigt die Seite **Clustering** nach der Definition eines Clusters. Das Gerät, auf dem der Cluster definiert ist, wird das erste Mitglied im Cluster.

**Tabelle 1: Clustering > Registerkarte „Status“**

Element der Benutzeroberfläche	Beschreibung
Schaltfläche <b>Add Member</b>	Klicken Sie auf diese Schaltfläche, um ein IVE anzugeben, das dem Cluster beitreten soll. Diesen Schritt müssen Sie für jedes IVE durchführen, das Sie dem Cluster hinzufügen möchten.
Schaltfläche <b>Enable</b>	Klicken Sie auf diese Schaltfläche, um einen zuvor deaktivierten Knoten zu aktivieren. Wenn Sie einen Knoten wieder aktivieren, werden alle Statusinformationen auf dem Knoten synchronisiert.
Schaltfläche <b>Disable</b>	Klicken Sie auf diese Schaltfläche, um einen Knoten in einem Cluster zu deaktivieren. Der Knoten kommuniziert weiterhin mit dem Cluster.

**Tabelle 1: Clustering > Registerkarte „Status“** fortgesetzt

Element der Benutzeroberfläche	Beschreibung
Schaltfläche <b>Remove</b>	Klicken Sie auf diese Schaltfläche, um den oder die ausgewählten Knoten aus dem Cluster zu entfernen. Ein Knoten wird ausgewählt, indem Sie das Kontrollkästchen neben dem Namen aktivieren. Nachdem der Knoten entfernt wurde, wird er im eigenständigen Modus ausgeführt.
Spalte <b>Cluster Members</b>	Führt alle Knoten auf, die zu dem Cluster gehören. Sie können auf einen Knoten klicken, um seinen Namen und die Netzwerkeinstellungen zu ändern.
Spalte <b>Internal IP Address</b>	Gibt die interne IP-Adresse des Clustermitglieds an.
Spalte <b>External IP Address</b>	Gibt die externe IP-Adresse des Clustermitglieds an. Beachten Sie, dass diese Spalte nur die externe IP-Adresse des Clusterleiters enthält, es sei denn, Sie geben auf seiner eigenen Seite für Netzwerkeinstellungen eine andere Adresse für den Knoten an. Zum Öffnen dieser Seite klicken Sie in der Spalte <b>Cluster Members</b> auf den Namen des Knotens. Wenn Sie die externe IP-Adresse auf der Seite <b>Network &gt; Network Settings</b> ändern, wirkt sich die Änderung auf alle Clusterknoten aus.

**Tabelle 1: Clustering > Registerkarte „Status“** fortgesetzt

Element der Benutzeroberfläche	Beschreibung
Spalte <b>Status</b>	<p>Gibt den Status des Knotens an:</p> <ul style="list-style-type: none"><li>• <b>Enabled</b>—Der Knoten bearbeitet Benutzeranforderungen und nimmt an der Clustersynchronisierung teil.</li><li>• <b>Disabled</b>—Der Knoten bearbeitet keine Benutzeranforderungen und nimmt nicht an der Clustersynchronisierung teil.</li></ul> <hr/> <p><b>Hinweis:</b> Der Status eines Knotens wird als „eigenständig“ betrachtet, wenn der Knoten außerhalb eines Clusters bereitgestellt wird oder aus einem Cluster entfernt wurde.</p> <hr/>
Spalte <b>Connection</b>	<p>Gibt den Status der Verbindung des Knotens mit dem Cluster an. Der Status kann folgendermaßen lauten:</p> <ul style="list-style-type: none"><li>• <b>OK</b>—Der Knoten ist aktiver Bestandteil des Clusters.</li><li>• <b>Transitioning</b>—Der Knoten wechselt vom eigenständigen Status in den aktivierten Status.</li><li>• <b>Unreachable</b>—Der Knoten ist gegenwärtig offline, d. h. er kommuniziert nicht mit dem Cluster.</li></ul> <hr/>

## Registerkarte „Properties“

### ☑ Ändern von Clustereigenschaften oder Löschen eines Clusters

Auf dieser Registerkarte können Sie den Namen eines Clusters ändern, angeben, in welchem Modus ein Clusterpaar ausgeführt werden soll, Synchronisierungseinstellungen festlegen oder einen Cluster löschen.

#### So ändern Sie Clustereigenschaften

1. Wählen Sie in der Administratorkonsole eines aktiven Clustermitglieds die Registerkarte **Network > Clustering > Properties** aus.
2. Nehmen Sie die gewünschten Änderungen vor, und klicken Sie dann auf **Save Changes**.
  - Die Clusterbezeichnung können Sie im Feld **Cluster Name** ändern.
  - Um die Konfigurationseinstellung für ein Clusterpaar festzulegen, wählen Sie **Active/Passive** oder **Active/Active** aus. Für eine Aktiv/Passiv-Konfiguration geben Sie eine interne VIP (virtuelle IP-Adresse) und, sofern der externe Port aktiviert ist, eine externe VIP an.

---

**Hinweis:** Der Bereich **Configuration Settings** wird nur für Clusterpaare angezeigt.

---

- Wählen Sie die gewünschten Synchronisierungseinstellungen aus. Geben Sie dabei auch das zu verwendende Synchronisierungsprotokoll an und legen Sie fest, ob Protokollmeldungen synchronisiert werden sollen. Erläuterungen der Synchronisierungseinstellungen finden Sie auf Seite 233.

#### So löschen Sie einen Cluster

1. Wählen Sie in der Administratorkonsole eines aktiven Clustermitglieds die Registerkarte **Network > Clustering > Properties** aus.
2. Wählen Sie **Delete Cluster** aus. Nach Beendigung des Vorgangs werden alle Clusterknoten als eigenständige IVEs ausgeführt.

**NEOTERIS**  
Administrator Console [Help](#) | [Sign Out](#)

**System**

- Settings
- Appearance
- Certificates
- Import/Export
- Install Service Package

**Authentication & Authorization**

- Administrators
- Authentication Servers
- Authorization Groups
- Active Users

**Network**

- Network Settings
- Clustering
- Web Proxy
- SNMP

## Clustering

Status Properties

Type: Cluster Pair

Cluster Name:

Cluster Password:

Confirm Password:

### Configuration Settings

☐ Active/Passive configuration  
This is a high-availability failover mode, in which one IVE is active while the other is held as backup.

Internal VIP:

External VIP:

☒ Active/Active configuration  
This mode requires an external load-balancer.

### Synchronization Settings

Protocol: ☒ Unicast ☐ Multicast ☐ Broadcast

☒ Synchronize log messages

**Abbildung 108: Network > Clustering > Properties**

Die Registerkarte **Properties** enthält keinen Bereich **Configuration Settings** für einen Multi-Unit-Cluster.

## Menü „Network > Web Proxy“

### ☒ Angeben eines Webproxys

Auf dieser Registerkarte können Sie Einstellungen für den Webproxy festlegen.

#### So geben Sie einen Webproxy an:

1. Wählen Sie in der Administratorkonsole das Menü **Network > Web Proxy** aus.
2. Klicken Sie unter **Use Web Proxy** auf **Enabled**.
3. Geben Sie unter **Web Proxy Server Information** den Namen oder die IP-Adresse des Webproxyservers sowie die Portnummer ein, an der der Proxyserver Daten abfragt.
4. Aktivieren Sie unter **Unqualified hostnames** das Kontrollkästchen **Send requests specified without a domain name to the Web proxy**, falls URLs mit unvollständigen Hostnamen, wie zum Beispiel `http://host/xyz` anstelle von `http://host.domain.com/xyz`, an den Proxyserver weitergeleitet werden sollen.
5. Wählen Sie unter **Exceptions** Folgendes aus:
  - **All requests are sent to the Web proxy EXCEPT for the following domains**, wenn Sie bestimmte Domänen festlegen möchten, mit denen das Neoteris IVE eine **direkte** Verbindung herstellt. Das IVE leitet Hostnamen, die in der Liste **Domains** aufgeführt sind, *nicht* an den Webproxy weiter.
  - **No requests are sent to the Web proxy EXCEPT for the following domains**, wenn Sie bestimmte Domänen festlegen möchten, deren Anforderungen an den Webproxy weitergeleitet werden. Das IVE leitet Hostnamen, die in der Liste **Domains** aufgeführt sind, an den Webproxy weiter.

Nachdem Sie festgelegt haben, wie Anforderungen weitergeleitet werden sollen, müssen Sie die entsprechenden Domänen in der Liste **Domains** hinzufügen. Hierfür gibt es zwei Möglichkeiten:

- Als DNS-Domännennamen
- Als Kombination aus IP-Adresse + Netzmaske

Die Anwendungslogik liest den Hostnamenabschnitt eines URL als Zeichenfolge aus und vergleicht die Zeichenfolge anschließend mit den Einträgen in der Liste **Domains**.



**Beispiele:**

Ein Eintrag in der Liste **Domains** in der Form `alpha.com` entspricht URLs mit der Form `http://*.alpha.com/*` und `http://alpha.com/*`, wobei `*` eine beliebige Sequenz aus null oder mehr Zeichen ist.

Ein Eintrag in der Liste **Domains** in der Form `10.10.0.1/255.255.255.0` folgt der üblichen IP/Netzmaske-Semantik und entspricht URLs in der Form `http://10.10.0.NN/*`, wobei `NN` eine Zahl zwischen 1 und 254 und `*` eine beliebige Sequenz aus null oder mehr Zeichen ist.

---

**Hinweis:** Wenn Sie statt eines Bereichs eine bestimmte IP-Adresse eingeben möchten, müssen Sie als Netzmaske unbedingt `255.255.255.255` angeben.

---

---

**Wichtig:** Das IVE löst keine Domänennamen in IP-Adressen auf und führt kein Reverse-Lookup für IP-Adressen durch. Ein URL, die statt auf einen Hostnamen auf eine IP-Adresse verweist, wird nur dann vom Proxy durchgelassen, wenn die Domänenliste einen entsprechenden Eintrag enthält.

---

6. Klicken Sie auf **Save Changes**.

NEOTERIS

Administrator Console

Help | Sign Out

System

Authentication & Authorization

Network

○ Settings

○ Appearance

○ Certificates

○ Import/Export

○ Install Service Package

○ Secure Meetings

○ Administrators

○ Authentication Servers

○ Authorization Groups

○ Import Users

○ Active Users

○ Network Settings

○ Clustering

○ Web Proxy

○ Email Settings

○ SNMP

Web Proxy

Save Changes

Reset

Use Web Proxy

☐ Enabled

☒ Disabled

Web Proxy Server Information

Address:

Port:

Address can be a fully qualified domain name (e.g. "proxy.net") or an IP

Unqualified Hostnames

☐ Send requests specified without a domain name (e.g. "servername", not "servername.domain.com") to the web proxy

Exceptions

☒ All requests are sent to the web proxy server EXCEPT for the following domains

☐ No requests are sent to the web proxy server EXCEPT for the following domains

Update

Add Domain

Name:

example: "domain.com", accepts \* or ? wildcards

See the documentation for info about adding IP address ranges.

Add ->

Remove

Domains

(none specified)

Save Changes?

Save Changes

Reset

Abbildung 109: Network > Web Proxy

## Menü „Network > Email Settings“

### ☒ Festlegen von IMAP/POP/SMTP-Mailservern und von Einstellungen für die Benutzerauthentifizierung

Das IVE unterstützt mehrere Mailserver. Sie können festlegen, dass alle Benutzer einen Standardmailserver verwenden müssen, oder Sie können Benutzern die Möglichkeit geben, einen benutzerdefinierten SMTP- und IMAP- oder POP-Mailserver anzugeben. Wenn Sie Benutzern das Festlegen eines benutzerdefinierten Mailservers ermöglichen, müssen diese die Servereinstellungen über das IVE vornehmen. Der IVE-Server verwaltet die E-Mail-Benutzernamen, um Namenskonflikte zu vermeiden.

---

**Hinweis:** Für das Verfahren zur E-Mail-Authentifizierung können Sie eine von drei Optionen festlegen, die nachfolgend in Schritt 6 erläutert werden. Bei jeder Option müssen die Benutzer bestimmte Konfigurationsschritte auf dem IVE durchführen.

---

#### So aktivieren Sie die Funktion für sichere Client-E-Mail für eine Gruppe

1. Wählen Sie in der Administratorkonsole das Menü **Authentication & Authorization > Authorization Groups** und anschließend eine Gruppe aus.
2. Wählen Sie aus den Gruppenregisterkarten **Email Client** aus.
3. Klicken Sie unter **Enable Secure Email Client** auf **Enabled** und dann auf **Save Changes**.
4. Wählen Sie im Hauptmenü **Network > Email Settings** aus.
5. Klicken Sie unter **Email Proxy Support** auf **Enabled**. Diese systemweite Option legt fest, dass das IVE als Mailserverproxy verwendet wird. Darüber hinaus müssen Sie die Option **Secure Email Client** auf Gruppenebene aktivieren.
6. Wählen Sie unter **Email Authentication Mode** die Authentifizierungsoption für die Gruppe aus. Folgende Optionen stehen zur Verfügung:
  - **Use a Web-based email session (Standardeinstellung)**  
Benutzer müssen eine einmalige E-Mail-Einrichtung für das IVE vornehmen. Anschließend konfigurieren sie ihren E-Mail-Client so, dass der Benutzername und das Kennwort verwendet werden, die durch die E-Mail-Einrichtung für das IVE generiert werden. Es empfiehlt sich, dass die Benutzer sich an dem IVE anmelden, um eine E-Mail-Sitzung zu starten.

- **Use Neoteris authentication AND mail server authentication**

Benutzer konfigurieren ihren E-Mail-Client so, dass die folgenden Anmeldeinformationen verwendet werden:

- **Benutzername:** Der normale Benutzername eines Benutzers für den Mailserver oder ein Benutzername, der beim E-Mail-Setup für das IVE generiert wird, wenn eine der folgenden Bedingungen zutrifft:
  - der Benutzer verfügt über mehrere Benutzernamen für den Mailserver
  - die Benutzernamen auf dem IVE-Server und dem Mailserver sind unterschiedlich
- **Kennwort:** Das IVE-Kennwort des Benutzers, gefolgt von einem benutzerdefinierbaren Trennzeichen für Anmeldeinformationen, gefolgt von dem Mailserverkennwort des Benutzers.

Benutzer müssen sich nicht am IVE anmelden, um E-Mail zu verwenden.

- **Use mail server authentication only**

Benutzer konfigurieren ihren E-Mail-Client so, dass ihre normalen Mailserver-Benutzernamen und -Kennwörter verwendet werden. Benutzer müssen sich nicht am IVE anmelden, um E-Mail zu verwenden oder zu konfigurieren.

---

**Hinweis:** Die Benutzer können ihre Benutzernamen und Kennwörter für E-Mail problemlos auf der Seite **Email Setup** ermitteln.

---

7. Geben Sie unter **Default Server Information** Ihre Mailserverdaten an. Das IVE fungiert als E-Mail-Proxy für diesen Server.

---

**Wichtig:** Sie können nur einen Standardmailserver angeben. Wenn Benutzer E-Mail-Nachrichten von mehreren SMTP- und POP- oder IMAP-Servern abrufen müssen, bieten Sie ihnen die Möglichkeit, weitere Mailserver zu definieren.

---

8. Klicken Sie auf **Save Changes**.

### Hinweis:

Wenn Sie Benutzern die Festlegung benutzerdefinierter Server ermöglichen, müssen sie diese Informationen auf ihrer IVE-Seite **Email Setup** eingeben.

NEOTERIS

Administrator Console

Help | Sign Out

System

Authentication & Authorization

Network

Settings

Appearance

Certificates

Import/Export

Install Service Package

Secure Meetings

Administrators

Authentication Servers

Authorization Groups

Import Users

Active Users

Network Settings

Clustering

Web Proxy

Email Settings

SNMP

Email Settings

Save Changes

Reset

Email Proxy Support

☒ Enabled

☐ Disabled

Note:

This enables the secure email proxy service. To allow users to use this service, you must also enable this feature on the User [Messaging](#) page.

Email Authentication Mode

☐ Web-based email session

Users sign in to the IVE to start an email session. Users must also generate username and password credentials, and enter them into their email client.

☐ Allow email password caching (if unchecked, users must enter their email password whenever starting an email session)

☒ Combined IVE and mail server authentication

Users do not need to sign in to the IVE to use email, but may need to sign in for initial setup to specify alternative mail servers or generate a unique username, which must then be entered into their email client. For password, users enter a combination of their IVE and mail server passwords, delimited by password separator defined below:

Password Separator: 

,

(comma)

☐ Mail server authentication only

Users do not need to sign in to the IVE to use email, and simply configure their email client with their email username and password as normal. Users who are not using the default mail server must sign in once to specify their email information. Name conflicts are also resolved in this way. This option is the least secure and is not recommended.

Default Server Information

SMTP Server: 

win2k.qa.danastreet.net

 Port: 

25

☒ Allow user to specify a custom SMTP server

POP Server: 

win2k.qa.danastreet.net

 Port: 

110

☒ Allow user to specify a custom POP server

IMAP Server: 

win2k.qa.danastreet.net

 Port: 

143

☒ Allow user to specify a custom IMAP server

Email Session Information

Idle Timeout: 

60

 minutes

Max. Session Length: 

720

 minutes

Abbildung 110: Network > Email Settings

## Menü „Network > SNMP“

Über diese Registerkarte können Sie ein Netzwerkverwaltungstool wie HP OpenView zum Überwachen des IVE als SNMP-Agent verwenden. Das IVE unterstützt SNMP v2, implementiert eine private MIB (Management Information Base) und definiert eigene Traps. Um die Verarbeitung dieser Traps in der Netzwerkverwaltungsstation zu ermöglichen, müssen Sie die Neoteris-MIB-Datei herunterladen und die entsprechenden Angaben zum Empfangen der Traps machen.

---

**Hinweis:** Zum Überwachen wesentlicher IVE-Systemstatistiken, beispielsweise der CPU-Auslastung, laden Sie die UC-Davis-MIB-Datei in Ihre SNMP-Managementanwendung. Sie erhalten die MIB-Datei im Internet unter folgender Adresse:  
<http://net-snmp.sourceforge.net/UCD-SNMP-MIB.txt>.

---

### So legen Sie SNMP-Einstellungen fest

1. Wählen Sie in der Administratorkonsole das Menü **Network > SNMP** aus.
2. Klicken Sie auf die Verknüpfung mit der **Neoteris MIB file**, um auf die MIB-Datei zuzugreifen, und speichern Sie die Datei dann im Browser unter einem Netzwerkpfad.
3. Führen Sie unter **Agent Properties** folgende Schritte durch:
  - Geben Sie in die Felder **System Name**, **System Location** und **System Contact** Informationen ein, die den IVE-Agenten beschreiben. (Optional.)
  - Geben Sie im Feld **Community** eine Zeichenfolge ein. (Erforderlich.)

---

**Hinweis:** Zum Abfragen des IVEs muss Ihre Netzwerkverwaltungsstation diese Zeichenfolge an das IVE senden. Um den SNMP-Daemon zu beenden, löschen Sie die Angaben im Feld **Community**.

---

4. Legen Sie unter **Traps** die Server fest, an die das IVE Traps senden soll, die es bei Eingabe folgender Daten generiert:
  - Der Hostname oder die IP-Adresse des Servers
  - Der Port, an dem der Server Daten abfragt (üblicherweise Port 162)
  - Die von der Netzwerkverwaltungsstation benötigte Community-Zeichenfolge (sofern vorhanden)

5. Gehen Sie in der Netzwerkverwaltungsstation folgendermaßen vor:
- 1 Laden Sie die Neoteris-MIB-Datei herunter.

2 Geben Sie die Community-Zeichenfolge an, die beim Abfragen des IVEs benötigt wird (siehe Schritt 3).

3 Konfigurieren Sie die Netzwerkverwaltungssoftware für den Empfang von IVE-Traps.

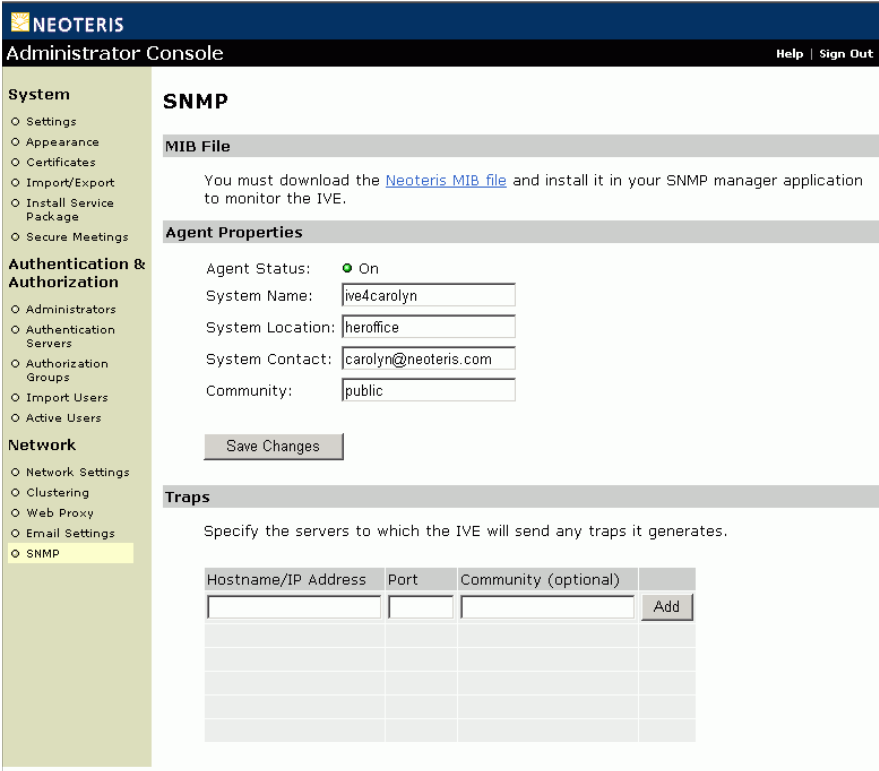


Abbildung 111: Network > SNMP





## Anhang A.

# Verwenden der seriellen Konsole von Neoteris

Die serielle Konsole von Neoteris bietet eine Oberfläche zum Durchführen der folgenden Vorgänge:

- Systemwiederherstellung durch ein Rollback in den vorherigen Zustand (2)
- Systemwiederherstellung durch Zurücksetzen des Geräts in den Werkszustand (4)
- Erstes Setup, das Sie bei der ersten Konfiguration des Computers oder nach dem Zurücksetzen des Geräts in den Werkszustand durchführen (7)
- Änderungen der Systeminformationen und Verwaltungsaufgaben (7), beispielsweise:
  - Anzeigen oder Festlegen der Netzwerkeinstellungen
  - Erstellen von Benutzernamen und Kennwörter für den Administrator
  - Aufheben von IP-Adressen-Beschränkungen für Administratoren
  - Anzeigen des Systemprotokolls
  - Ausführen eines Ping-Befehls auf einen Server
  - Verfolgen der Route zu einem Server
  - Entfernen aller statischen Routen
  - Entfernen der clientseitigen SSL-Authentifizierung für Administratoren

## ☒ Herstellen einer Verbindung mit der seriellen Konsole des IVE

Um Aufgaben über die serielle Konsole von Neoteris durchführen zu können, müssen Sie ein Konsolenterminal oder einen Laptop an das Neoteris-Gerät anschließen.

### **So stellen Sie eine Verbindung mit der seriellen Konsole des IVE her:**

1. Schließen Sie ein Nullmodem-Crossover-Kabel vom Konsolenterminal oder Laptop an das Neoteris IVE-Gerät an. Dieses Kabel ist im Lieferumfang des Geräts enthalten. Verwenden Sie kein einfaches serielles Kabel.

2. Konfigurieren Sie das Terminal oder die Terminalemulationssoftware (beispielsweise HyperTerminal) mit den folgenden Parametern für serielle Verbindungen:
  - 9600 Bit pro Sekunde
  - 8 Bit, keine Parität (8N1)
  - 1 Stopp-Bit
  - Keine Flusskontrolle
3. Drücken Sie **Eingeben**, bis die serielle Konsole von Neoteris angezeigt wird:

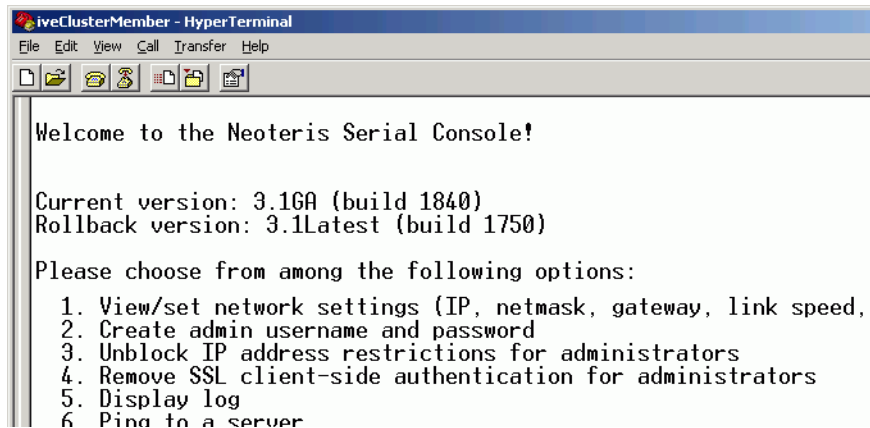


Abbildung 112: Neoteris Serielle Konsole

## ☒ Rollback zu einem vorherigen Systemzustand

Sie können das System über die Administratorkonsole in der Regel folgendermaßen in einen vorherigen Systemzustand zurückversetzen:

1. Navigieren Sie zu den zuvor gespeicherten System- und Benutzerkonfigurationsdateien, in denen die gewünschten Daten gespeichert sind.
2. Laden Sie die gewünschten Serverpakete unter „support.neoteris.com“ herunter.
3. Importieren Sie das gewünschte Serverpaket.

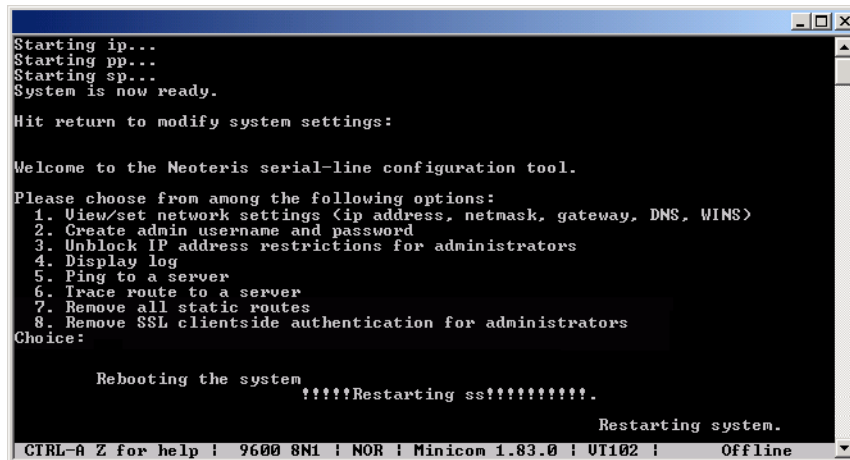
4. Importieren Sie die gewünschten System- und Benutzerkonfigurationsdateien.

Der Neoteris IVE-Server speichert die aktuellen Systemkonfigurationsinformationen und die des vorherigen Systemzustands. Wenn Sie das Serverpaket aktualisieren und Ihr Gerät in den vorherigen Zustand zurücksetzen möchten, empfehlen wir Ihnen, den zuvor aufgeführten Anweisungen zu folgen. Wenn Sie nicht auf die Administratorkonsole zugreifen können, stellen Sie eine Verbindung mit der seriellen Konsole her, um ein Rollback zum vorherigen Systemzustand durchzuführen.

Wenn Sie bisher noch keine Serveraktualisierung durchgeführt haben, gibt es keinen älteren Systemzustand, und die Option ist daher nicht verfügbar. Wenn Sie eine Serveraktualisierung durchgeführt haben, gehen alle System- und Benutzerkonfigurationsdaten, die nach der Aktualisierung erstellt wurden, verloren. Dies vermeiden Sie, indem Sie die aktuellen Konfigurationsdateien vor dem Rollback des Systems exportieren und anschließend wieder importieren.

**So führen Sie ein Rollback zum vorherigen Serverzustand durch:**

1. Stellen Sie eine Verbindung mit der seriellen Konsole her (siehe unter Seite 273).
2. Melden Sie sich in einem Browserfenster an der **Administratorkonsole** an.
3. Wählen Sie im Hauptmenü **General > Status** aus.
4. Klicken Sie auf der Seite **Status** auf **Reboot Now**, und wechseln Sie dann wieder zum Konsolenprogrammfenster zurück. Im Fenster werden Sie in einer Meldung informiert, dass das System neu gestartet wird.



```
Starting ip...
Starting pp...
Starting sp...
System is now ready.

Hit return to modify system settings:

Welcome to the Neoteris serial-line configuration tool.

Please choose from among the following options:
1. View/set network settings (ip address, netmask, gateway, DNS, WINS)
2. Create admin username and password
3. Unblock IP address restrictions for administrators
4. Display log
5. Ping to a server
6. Trace route to a server
7. Remove all static routes
8. Remove SSL clientside authentication for administrators
Choice:

Rebooting the system
!!!!Restarting ss!!!!!!!!!.

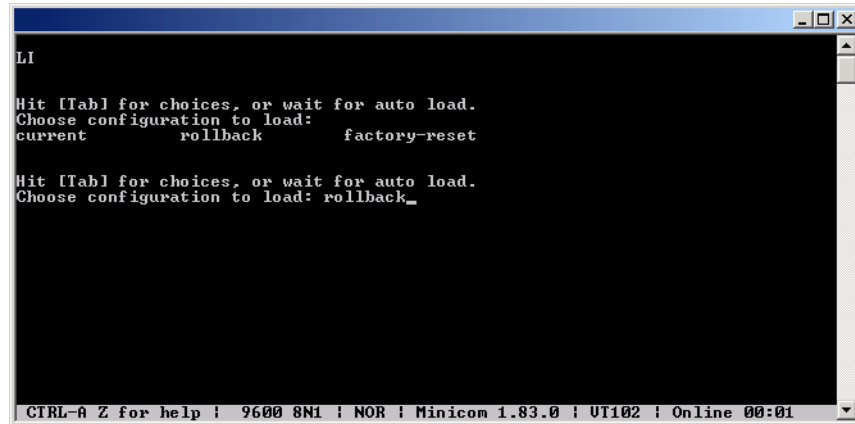
Restarting system.

CTRL-A Z for help ! 9600 8N1 ! NOR ! Minicom 1.83.0 ! UT102 ! Offline
```

**Abbildung 113: Neoteris Serielle Konsole**

Nach dem Klicken auf „Reboot Now“ auf der Seite General > Status.

5. Nach kurzer Zeit werden Sie aufgefordert, für die Auswahl von Optionen die **Tab-Taste** zu drücken. Drücken Sie die **Tab-Taste**. Wenn Sie gefragt werden, welche Konfiguration geladen werden soll, geben Sie **rollback** ein, und drücken Sie dann die **Eingabetaste**.



**Abbildung 114: Neoteris Serielle Konsole**

Nach dem Klicken auf „Reboot Now“ auf der Seite General > Status (zweiter Bildschirm).

---

**Hinweis:**

- Wenn Sie beim Auswählen länger als 5 Sekunden warten, wird automatisch die aktuelle Systemkonfiguration geladen. Sie müssen dann zurück in die Administratorkonsole wechseln und auf **Reboot Now** klicken, um den Vorgang erneut zu starten.
  - Wenn Sie bereits ein Systemrollback durchgeführt haben, ist die Rollbackoption erst wieder verfügbar, wenn Sie die Serversoftware erneut aktualisieren.
- 

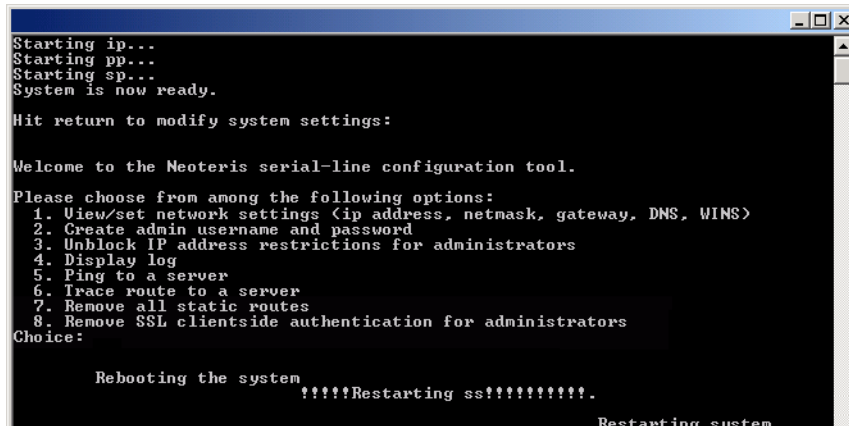
Der Rollbackstatus des Servers wird auf den Bildschirm ausgegeben. Wenn der Vorgang abgeschlossen ist, werden Sie zum Drücken der **Eingabetaste** aufgefordert, um die Systemeinstellungen zu ändern. Dadurch kehren Sie zu den Optionen für das erste Setup zurück. Wenn Sie die Dateneingabe abgeschlossen haben, schließen Sie einfach das Programmfenster.

## ☑ Zurücksetzen des Neoteris-Geräts auf die Werkseinstellungen

Es kann im Ausnahmefall erforderlich sein, das Neoteris-Gerät auf die ursprünglichen Werkseinstellungen zurückzusetzen. Bevor Sie diese tiefgreifende Systemwiederherstellungsoption ausführen, wenden Sie sich bitte unter der Adresse „help@support.neoteris.com“ an den Neoteris-Support. Vor dem Zurücksetzen auf die Werkseinstellungen sollten Sie nach Möglichkeit die aktuellen System- und Benutzerkonfigurationsdaten exportieren.

### So setzen Sie das Gerät auf die Werkseinstellungen zurück:

1. Stellen Sie eine Verbindung mit der seriellen Konsole her (siehe unter Seite 273).
2. Melden Sie sich in einem Browserfenster an der **Administratorkonsole** an.
3. Wählen Sie im Hauptmenü **General > Status** aus.
4. Klicken Sie auf der Seite **Status** auf **Reboot Now**, und wechseln Sie dann wieder zum Konsolenprogrammfenster zurück. Im Fenster werden Sie in einer Meldung informiert, dass das System neu gestartet wird.



```
Starting ip...
Starting pp...
Starting sp...
System is now ready.

Hit return to modify system settings:

Welcome to the Neoteris serial-line configuration tool.

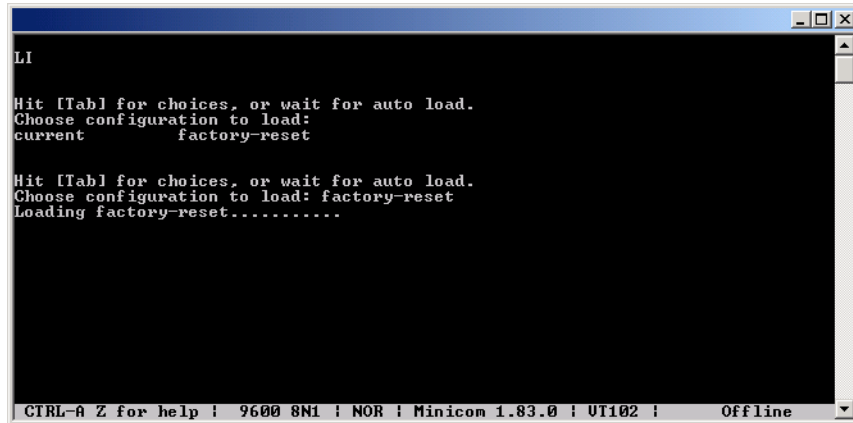
Please choose from among the following options:
1. View/set network settings (ip address, netmask, gateway, DNS, WINS)
2. Create admin username and password
3. Unblock IP address restrictions for administrators
4. Display log
5. Ping to a server
6. Trace route to a server
7. Remove all static routes
8. Remove SSL clientside authentication for administrators
Choice:

Rebooting the system
!!!!Restarting ss!!!!!!!.
Restarting system.
```

**Abbildung 115: Neoteris Serielle Konsole**

Nach dem Klicken auf „Reboot Now“ auf der Seite General > Status.

5. Nach kurzer Zeit werden Sie aufgefordert, für die Auswahl von Optionen die **Tab-Taste** zu drücken. Drücken Sie die **Tab-Taste**. Wenn Sie gefragt werden, welche Konfiguration geladen werden soll, geben Sie `factory-reset` ein, und drücken Sie dann die **Eingabetaste**.



**Abbildung 116: Neoteris Serielle Konsole**

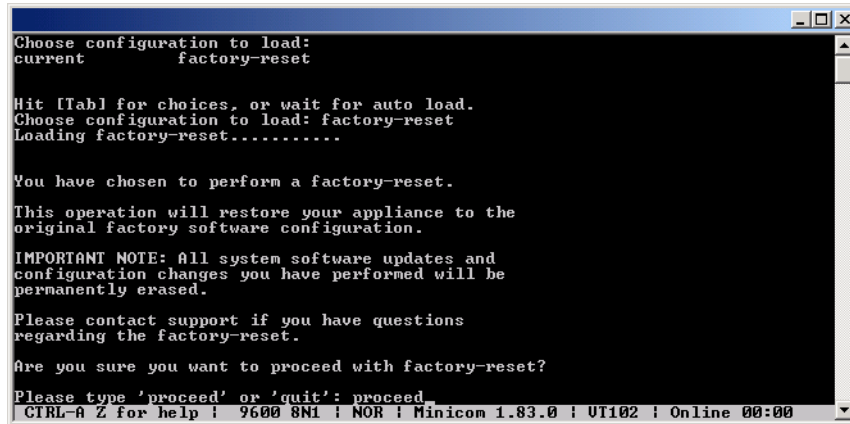
Nach dem Klicken auf „Reboot Now“ auf der Seite General > Status (zweiter Bildschirm).

---

**Hinweis:** Wenn Sie beim Auswählen länger als 5 Sekunden warten, wird automatisch die aktuelle Systemkonfiguration geladen. Sie müssen dann zurück in die Administratorkonsole wechseln und auf **Reboot Now** klicken, um den Vorgang erneut zu starten.

---

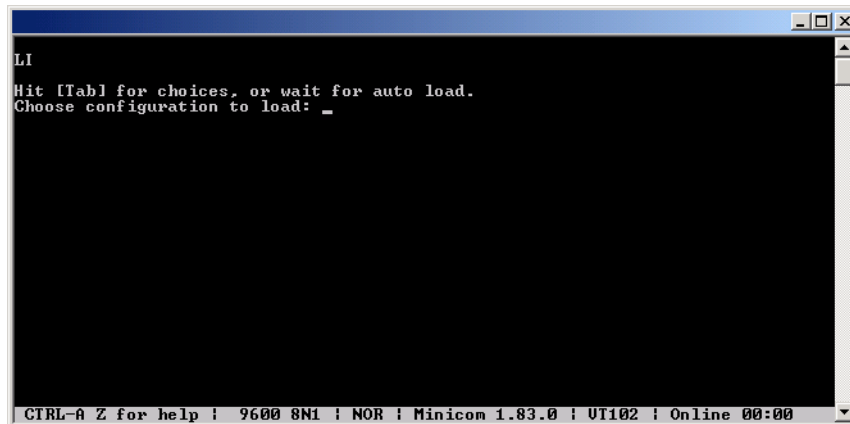
6. Wenn Sie aufgefordert werden, das Zurücksetzen auf die Werkseinstellungen zu bestätigen, geben Sie `proceed` ein, und drücken Sie dann die **Eingabetaste**.



**Abbildung 117: Neoteris Serielle Konsole**

Hier wurde das Zurücksetzen auf die Werkseinstellungen ausgewählt.

Das System beginnt mit dem Zurücksetzen des Geräts auf die Original-einstellungen und gibt dabei mehrere Bildschirme mit Daten aus. Nach einigen Minuten werden Sie aufgefordert, für die Auswahl von Konfigurationsoptionen die **Tab-Taste** zu drücken.



**Abbildung 118: Neoteris Serielle Konsole**

Nach dem Zurücksetzen auf die Werkseinstellungen.

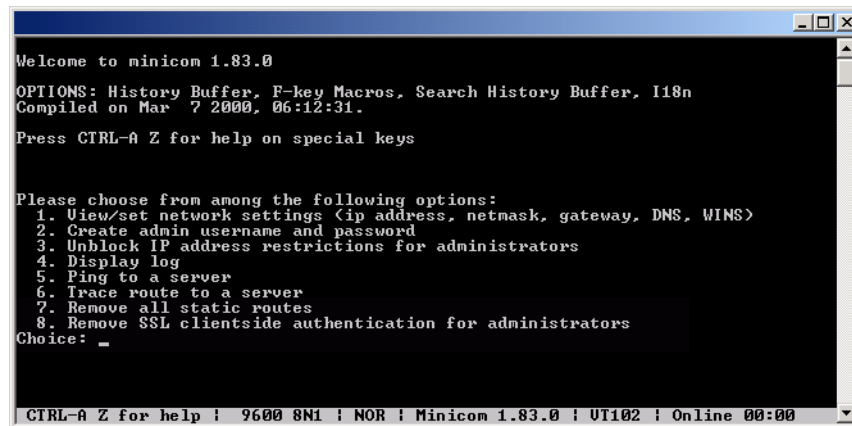
7. Wenn Sie zum Drücken der **Tab-Taste** aufgefordert werden, gibt es folgende Möglichkeiten:
  - Warten Sie den automatischen Start der Standardoption ab (current), oder
  - drücken Sie die **Tab-Taste**, geben Sie `current` ein, und drücken Sie dann die **Eingabetaste**.

Sie werden dann aufgefordert, die ursprünglichen Konfigurationseinstellungen des Geräts einzugeben. Detaillierte Informationen zur Vorgehensweise können Sie dem Installationshandbuch entnehmen, das dem Gerät beiliegt. Dieses Handbuch steht auch auf der Neoteris-Supportsite im PDF-Format zur Verfügung.

Nach dem Abschluss des Initialisierungsvorgangs können Sie auf das neueste Serverpaket aktualisieren und die gespeicherten System- und Benutzerkonfigurationsdateien importieren, um zum letzten funktionstüchtigen Zustand des Geräts zurückzukehren.

## ☒ Durchführen gängiger Wiederherstellungsvorgänge

Wenn Sie den Administratorbenutzernamen und/oder das Administrator Kennwort vergessen, sich aufgrund von IP-Einschränkungen selbst aus dem Gerät ausgeschlossen oder die IP-Adresse des Neoteris-Geräts geändert haben und das Gerät nicht mehr erreichen können, können Sie die Geräteeinstellungen über die serielle Konsole ändern. Folgen Sie einfach den Anweisungen unter „Herstellen einer Verbindung mit der seriellen Konsole des IVE“ auf Seite 273, und wählen Sie dann den gewünschten Konfigurationsvorgang aus.



```

Welcome to minicom 1.83.0
OPTIONS: History Buffer, F-key Macros, Search History Buffer, I18n
Compiled on Mar  7 2000, 06:12:31.

Press CTRL-A Z for help on special keys

Please choose from among the following options:
 1. View/set network settings (ip address, netmask, gateway, DNS, WINS)
 2. Create admin username and password
 3. Unblock IP address restrictions for administrators
 4. Display log
 5. Ping to a server
 6. Trace route to a server
 7. Remove all static routes
 8. Remove SSL clientside authentication for administrators
Choice: _

CTRL-A Z for help | 9600 8N1 | NOR | Minicom 1.83.0 | UT102 | Online 00:00
  
```

**Abbildung 119: Neoteris Serielle Konsole**  
Systemverwaltungsvorgänge



# Index

## A

- Ablaufverfolgungsdatei (zum Debuggen) 26
- Access Control (Unterregisterkarte),
  - Authorization Groups (Menü) > Web (Registerkarte) 158
- ACE/Agent-Konfigurationsdatei 117
- ACE/Server
  - Konfigurationsschritte 116
  - Übersicht 78
- ACLs & Bookmarks (Registerkarte),
  - Import/Export (Menü) 62
- Active Directory-Server
  - Konfigurationsschritte 106
  - Übersicht 75
- Active Users (Menü), Verwenden von
  - Aufgaben 220, 223
- Address Restrictions (Unterregisterkarte)
  - Administrators (Menü) > Authentication (Registerkarte) 89
  - Authorization Groups (Menü) > Authentication (Registerkarte) 138
- Administrator
  - authentifizieren 87
  - Benutzeradministrator 104
- Administratorengruppe
  - Anmeldeeinschränkungen
    - nach IP 89
    - nach Zertifikat 91
  - Authentifizierungsserver für 87
  - Beschreibung 73
  - Konten
    - bearbeiten 85
    - erstellen 83
    - löschen 85
    - suchen 86
    - verwalten 82
  - Sitzungszeitbegrenzungen 86
- Administratorkonsole, Clustermittglieder
  - hinzufügen 254
- Administrators (Menü),
  - Konfigurationsaufgaben 82
- Aktiv/Aktiv-Cluster
  - Abbildung 231
  - Übersicht über die Bereitstellung 230
- Aktiv/Passiv-Cluster
  - Abbildung 229
  - Übersicht über die Bereitstellung 229
- Aktualisierungsoption
  - Secure Email Client 176
  - Sicherer Terminalzugriff 179
- Anmeldeinformationen, Benutzer 10
- Anmeldung
  - Autorisierungsmodus 33
  - Einzelanmeldung mit Netegrity SiteMinder 81
  - Kennwortlänge 10
  - Optionen
    - Administratoreinschränkungen 89, 91
    - Benutzereinschränkungen 138, 139, 142, 145
    - Systemweite Einschränkungen 32
  - Seite
    - anpassen 36
- Appearance (Menü),
  - Konfigurationsaufgaben 36
- Applet Certificate (Registerkarte), Certificates (Menü) 54
- Archivierungsplanung 24
- Archiving (Registerkarte), Settings (Menü) 24
- ARP-Befehl 30
- Authentication & Authorization (Menüs)**
  - Active Users 220, 223
  - Administrators 82
  - Authentication Servers 92
  - Authorization Groups 126
- Authentication Server (Unterregisterkarte)
  - Administrators (Menü) > Authentication (Registerkarte) 87
  - Authorization Groups (Menü) > Authentication (Registerkarte) 137
- Authentication Servers (Menü),
  - Konfigurationsaufgaben 92
- Authentifizierung
  - unterstützte Server 75
  - von Administratoren 87
  - Vorgangsbeschreibung 72

- Authentifizierungseinstellungen
  - für Administratoren 89, 91
  - für Benutzer 138, 142, 145
- Authentifizierungsserver
  - Übersicht 72
  - Zuordnung von Servern zu Gruppen 137
- Authorization Groups (Menü),  
Konfigurationsaufgaben 126
- Authorization Mode (Unterregisterkarte),  
Settings (Menü) > Sign-In Options  
(Registerkarte) 33
- Autorisierungsgruppe
  - Anmeldeeinschränkungen
    - nach Browser 140
    - nach IP 138
    - nach Zertifikat 142, 144, 145
  - benutzerdefinierte Autorisierungsgruppe  
erstellen 74
  - Lesezeichen
    - Einrichten sicherer Terminalsitzungen 185
    - für das Web erstellen 161
    - unter UNIX erstellen 174
    - unter Windows erstellen 170
  - Roamingfunktionen für mobile Benutzer 133
  - Sitzungszeitbegrenzungen 133
  - Übersicht 73
  - Windows-Ressourcenzugriffssteuerung 167
  - Zugriffssteuerung für Webserver 158
  - Zuordnung von Servern zu Gruppen 137
  - Zusammenfassung der Einstellungen 127
- Autorisierungsmodus, systemweite  
Anmeldung 33

## B

- Befehle, UNIX 30
- Begrüßungsnachricht, Bookmarks (IVE-  
Seite) 37
- Benutzer
  - Anmeldeeinschränkungen
    - nach Browser 139
    - nach Zertifikat 142, 145
  - „Benutzeradministrator“ 104
  - Beständigkeit von  
Anmeldeinformationen 135
  - clientseitiges Zertifikat erforderlich 42, 52
  - Codesignaturzertifikat für 54

- Daten
  - exportieren 64
  - importieren 64
- Kennwortlänge 10
- Konfigurieren von PCs für 201, 202
- Konten
  - erstellen 101
  - exportieren 60
  - importieren 61
  - suchen 103
  - verwalten 102
- Profildaten 232
- Roamingfunktionen 133
- Sitzungsdaten 232
- Sitzungszeitbegrenzungen 133
- Überwachen von Sitzungen 223
- Vermittlung von Anmeldeinformationen 10
- Benutzergruppe
  - Beschreibung 74
- Benutzeroberfläche
  - anpassen für Endbenutzer 36
- Bookmarks (Seite), anpassen für  
Endbenutzer 37
- Bookmarks (Unterregisterkarte), Authorization  
Groups (Menü) > Web (Registerkarte) 161
- Browser
  - Anmeldeeinschränkungen, Benutzer 139
  - Unterstützung für Cachesteuerung 15
- Browser Restrictions (Unterregisterkarte),  
Authorization Groups (Menü)>  
Authentication (Registerkarte) 139
- Browsing
  - im Web zulassen 148

## C

- CA Certificate (Registerkarte), Certificates  
(Menü) 52
- Cache, Regeln 13
- Cache-Control  
No-Store 13
- Certificate (Unterregisterkarte)
  - Administrators (Menü) > Authentication  
(Registerkarte) 91
  - Authorization Groups (Menü)>  
Authentication (Registerkarte) 142, 144
- Certificates (Menü),

- Konfigurationsaufgaben 41
- Citrix NFuse
  - Ändern von Parametern für J-SAM 215
  - Liste unterstützter Versionen 214
  - Übersicht 214
  - Unterstützung aktivieren 183
- Citrix NFuse (J-SAM) (Unterregisterkarte),
  - Authorization Groups (Menü) > Applications (Registerkarte) 214
- Clientseitige Java-Applets
  - Angeben von Verbindungen 163
  - zulassen 149
- Cluster
  - aktiv/aktiv 230
  - aktiv/passiv 229
  - aktualisieren 256
  - definieren und initialisieren 247
  - Eigenschaften ändern 262
  - konfigurieren, Übersicht 227
  - löschen 262
  - Status, Definition 259
  - über die Administratorkonsole hinzufügen 254
  - über serielle Konsole hinzufügen 249
  - verwalten 257
- Clustering (Menü),
  - Konfigurationsaufgaben 247
- Clusterpaar
  - Anforderungen 247
  - Definition 227
- Commands (Unterregisterkarte), Settings (Menü) > Debugging (Registerkarte) 30
- Configuration (Registerkarte), Import/Export (Menü) 58
- Content Caching (Unterregisterkarte), Settings (Menü) > Security (Registerkarte) 13
- Cookies, Behandlung ändern 149

## D

- Datei
  - Zugriffsstatistik 22
  - Zugriffssteuerung zum Durchsuchen 164
- Dateiserver, codieren 35
- Datenbank für Authentifizierung 75
- Debugging
  - Ablaufverfolungsdatei 26
  - remote 31

- Snapshotdatei 27
- TCP-Sicherungsdatei 28
- UNIX-Befehle 30
- Dienstpaket
  - installieren 66
- DMZ-Schnittstelle 241
- DNS
  - für externen Port 241
  - für internen Port 240
  - Konfigurieren für J-SAM 201
- Durchgangssproxy
  - Angeben von Anwendungen für 153
  - Beschreibung 150
- Durchsuchen
  - Probleme (Web) 26
  - Symbolleiste
    - Abbildung 36
    - Symbol ändern 37

## E

- Einschränkungen
  - Administratoranmeldung 91
  - Benutzeranmeldung 142, 145
  - systemweite Anmeldung 32
- Email Client (Registerkarte), Authorization Groups (Menü) 176
- Email Settings (Menü),
  - Konfigurationsaufgaben 267
- E-Mail-Einstellungen
  - Konfigurationsoptionen 267
- Encoding (Registerkarte), Settings (Menü) 35
- External Port (Registerkarte), Network Settings (Menü) 241

## G

- Gateway
  - für externen Port 241
  - für internen Port 240
- General (Registerkarte)
  - Appearance (Menü) 36
  - Secure Meetings (Menü) 68
  - Settings (Menü) 6
- General (Unterregisterkarte)
  - Authorization Groups (Menü) > Applications (Registerkarte) 178

- Authorization Groups (Menü) > Files (Registerkarte) 164
- Authorization Groups (Menü) > Web (Registerkarte) 148
- Settings (Menü) > Security (Registerkarte) 9
- Geschlossene Richtlinie
  - Web 158
  - Windows-Ressourcen 167

## H

- Herunterfahren des IVE-Servers 6
- Hilfe, an Support wenden xiii
- Hilfeschaltfläche 37
- Hostnamen, lokal auflösen 245
- Hostzuordnung
  - für Client-/Serveranwendungen 183
  - für MS Exchange 184

## I

- IMAP-Mailserver 267
- Import/Export (Menü),
  - Konfigurationsaufgaben 58
- Install Service Package (Menü),
  - Konfigurationsaufgabe 66
- Installation
  - Kontaktaufnahme mit Support, Hilfe xiii
- Internal Port (Registerkarte), Network Settings (Menü) 240
- Internet Explorer, ausführen einer JVM 54
- IP-Adresse
  - Anmeldeeinschränkungen für Administratoren 89
  - Anmeldeeinschränkungen für Benutzer 138
  - für externen Port 241
  - für internen Port 240
- IVE
  - Erstellen einer ACE/Agent-Konfigurationsdatei für 116
  - in LAN (Abbildung) 2
  - Konfigurieren als SiteMinder-Webagent 123
  - Konfigurieren von RADIUS zum Erkennen von 114

## J

- Java Socket ACL (Unterregisterkarte),
  - Authorization Groups (Menü) > Web (Registerkarte) 163
- Java-Applets
  - Angaben von Verbindungen 163
  - ausführen über MS und SUN JVM 54
  - zulassen 149
- JavaSoft-Zertifikat 54

## K

- Kennwortlänge 10
- Knoten, Cluster 257
- Konfiguration, Systemaktualisierung xiii
- Konfigurationsdatei
  - ACLs und Lesezeichen exportieren 64
  - ACLs und Lesezeichen importieren 64
  - lokale Benutzerkonten exportieren 60
  - lokale Benutzerkonten importieren 61
  - System exportieren 58
  - System importieren 59
- Konsole, seriell 273

## L

- LAN, Netzwerkeinstellungen ändern 240, 241
- LDAP-Server
  - Konfigurationsschritte 108
  - Übersicht 76
- Lesezeichen
  - Einrichten sicherer Terminalsitzungen 185
  - exportieren 64
  - für das Web erstellen 161
  - importieren 64
  - Java-Applet erforderlich 162
  - unter UNIX erstellen 174
  - unter Windows erstellen 170
- License (Registerkarte), Settings (Menü) 7
- Lizenzbeschreibung 7
- Lokaler Authentifizierungsserver
  - Konfigurationsschritte 92
  - Übersicht 75

**Lotus Notes**

- Abbildung 211
- Festlegen zulässiger Server für J-SAM 211
- Konfigurieren eines Clients 213
- Übersicht 210

- Lotus Notes (J-SAM) (Unterregisterkarte),  
Authorization Groups (Menü) > Applications  
(Registerkarte) 210

**M**

- Mail, Nutzungsstatistik zu Spitzenzeiten 22
- Mailserver, konfigurieren 267
- Meetings (Registerkarte), Authorization Groups  
(Menü) 216
- Members (Registerkarte), Administrators  
(Menü) 82
- Menü

- Authentication & Authorization > Active  
Users 220, 223
- Authentication & Authorization >  
Administrators 82
- Authentication & Authorization >  
Authentication Servers 92
- Authentication & Authorization >  
Authorization Groups 126
- Network > Clustering 247
- Network > Email Settings 267
- Network > Network Settings 240
- Network > SNMP 270
- Network > Web Proxy 264
- System > Appearance 36
- System > Certificates 41
- System > Import/Export 58
- System > Install Service Package 66
- System > Secure Meetings 67
- System > Settings 5

- Microsoft Authenticode-Zertifikat 54

**MS Exchange**

- Abbildung 206
- Aktualisierungen der Windows-  
Registrierung 207
- automatische Hostzuordnung 184
- Festlegen zulässiger Server für J-SAM 207
- Übersicht 205

- MS Exchange (J-SAM) (Unterregisterkarte),  
Authorization Groups (Menü) > Applications  
(Registerkarte) 205

**N**

- Neoteris Support, Zusammenarbeit mit 26–31
- Neoteris-Support xiii
- Netegrity SiteMinder-Server
  - Einzelanmeldung 81
  - Konfigurationsschritte 119, 123
  - Übersicht 79
- Netscape, ausführen einer JVM 54

**Network (Menüs)**

- Clustering 247
- Email Settings 267
- Network Settings 240
- SNMP 270
- Web Proxy 264
- Network Connect (Unterregisterkarte),  
Authorization Groups (Menü) > General  
(Registerkarte) 129
- Network Settings (Menü),  
Konfigurationsaufgaben 240
- Netzmaske
  - für externen Port 241
  - für internen Port 240
- Netzwerk, Angeben von lokal aufzulösenden  
Hostnamen 245
- Netzwerk, statische Routen angeben 243
- Netzwerkeinstellungen, ursprüngliche 226
- Netzwerkpakete, Abhören mit Sniffer-  
Programm 28

- Neu starten des IVE-Servers 6

**Neuschreiben**

- Option für den Durchgangssproxy 150, 153
- Option zum selektiven  
Neuschreiben 150, 152

**NIS-Server**

- Konfigurationsschritte 112
- Übersicht 76

- nslookup-Befehl 30

**O**

- Offene Richtlinie  
Web 158

- Windows-Ressourcen 167
- Options (Unterregisterkarte), Authorization Groups (Menü) > General (Registerkarte) 135
- Overview (Unterregisterkarte), Authorization Groups (Menü) > General (Registerkarte) 127

## P

- ping-Befehl 30
- POP-Mailserver 267
- Port
  - externen ändern 241
  - internen ändern 240
- Pragma
  - No-Cache (PNC) 13
- Privater Schlüssel 43
- Properties (Registerkarte), Clustering (Menü) 262

## R

- RADIUS-Server
  - Konfigurationsschritte 113
  - Übersicht 77
- Regeln
  - Browserzugriffssteuerung 140
  - Cachesteuerung 13
  - Zuordnung von Benutzern zu Gruppen 92
- Regeln für die Zwischenspeicherung von Inhalten 13
- Remote Debugging (Unterregisterkarte), Settings (Menü) > Debugging (Registerkarte) 31
- Restrictions (Unterregisterkarte), Settings (Menü) > Sign-in Options (Registerkarte) 32

## S

- Schedule (Registerkarte), Secure Meetings (Menü) 70
- Schlüssel 43
- „sdconf.rec“ generieren 117
- Secure Application Manager
  - Abbildung, Java-Version 196

- Abbildung, Windows-Version 188
- Ändern von Citrix NFuse-Parametern 215
- Angeben von MS Exchange-Servern 207
- Anwendungen, für J-SAM konfigurieren 197
- Anwendungen, für W-SAM konfigurieren 189
- Festlegen von Lotus Notes-Servern 211
- Hosts, für W-SAM konfigurieren 189
- Testen von J-SAM 203
- vs. Aktualisierungsoption für den Secure Email Client 176
- zusätzliche J-SAM-Optionen 181
- Secure Application Manager (J-SAM) (Unterregisterkarte), Authorization Groups (Menü) > Applications (Registerkarte) 193
- Secure Application Manager (W-SAM) (Unterregisterkarte), Authorization Groups (Menü) > Applications (Registerkarte) 187
- Secure Email Client
  - vs. Aktualisierungsoption für Secure Application Manager 176
- Secure Email Client, Übersicht 176
- Secure Meetings (Menü), Konfigurationsaufgaben 67
- Selektives Neuschreiben
  - Beschreibung 150
  - Konfigurieren von Hosts für 152
- Serielle Konsole
  - Clustermmitglieder hinzufügen 249
  - für systembezogene Aufgaben verwenden 273
- Server
  - ACE/Server 78
  - Active Directory 75
  - für Authentifizierung verwendete Typen 75
  - Instanz
    - ACE/Server 116
    - Active Directory 106
    - definieren (grundlegende Schritte) 92
    - LDAP 108
    - lokale Authentifizierung 75
    - Netegrity SiteMinder 119, 123
    - NIS 112
    - RADIUS 113
    - Windows NT-Domäne 106
  - LDAP 76
  - Lizenz für IVE eingeben 7
  - Netegrity SiteMinder 79
  - NIS 76

- Protokoll anzeigen 18
- RADIUS 77
- Software, Versionsüberwachung 11
- Windows NT-Domäne 75
- Server Certificate (Registerkarte), Certificates (Menü) 42
- Session (Registerkarte), Administrators (Menü) 86
- Session (Unterregisterkarte), Authorization Groups (Menü) > General (Registerkarte) 133
- Settings (Menü) > Log (Registerkarte) 18
- Settings (Menü), Konfigurationsaufgaben 5
- Settings (Unterregisterkarte), Log (Menü) 18
- Sicherer Terminalzugriff, Erstellen von Lesezeichen 185
- Sicherheitseinstellungen ändern 9
- Sign-in Page (Registerkarte), Appearance (Menü) 38
- Sitzungscookie, Beständigkeit (IVE) 135
- Sitzungszeitbegrenzungen
  - Administrator 86
  - Benutzer 133
- SMSESSION-Cookies 80
- SMTP-Mailserver 267
- Snapshotdatei (zum Debuggen) 27
- SNMP (Menü), Konfigurationsaufgaben 270
- SNMP-Einstellungen, festlegen 270
- Software
  - installieren 66
  - Versionsüberwachung 11
- SSL
  - navigieren zu Sites 10
  - zulässige Verschlüsselungsstärke 10
  - zulässige Version 10
- Startseite, anpassen für alle Benutzer 36
- State (Unterregisterkarte), Settings (Menü) > Debugging (Registerkarte) 27
- Static Routes (Registerkarte), Network Settings (Menü) 243, 245
- Statistics (Registerkarte), Settings (Menü) 22
- Statistik, Verwendung 22
- Status (Registerkarte), Clustering (Menü) 257
- Statussynchronisierung 232
- Symbol, Symboleiste zum Durchsuchen 37
- syslog, Ereignisse protokollieren 18
- System
  - Daten archivieren 24
  - Debugging 26, 27, 28, 30, 31

- herunterfahren 6
- Konfiguration exportieren 58
- Konfiguration importieren 59
- neu starten 6
- Protokoll anzeigen 18
- Rollback 273–280
- Software installieren 66
- Statistik anzeigen 22
- Status anzeigen 6
- Statusdaten, Beschreibung 232
- verbundene Server, Ping-Befehl senden 6
- Zeit einstellen 16
- System** (Menüs)
  - Appearance 36
  - Certificates 41
  - Import/Export 58
  - Install Service Package 66
  - Secure Meetings 67
  - Settings 5

## T

- TCP Dump (Unterregisterkarte), Settings (Menü) > Debugging (Registerkarte) 28
- TCP-Sicherungsdatei (zum Debuggen) 28
- Terminal Sessions (Unterregisterkarte), Authorization Groups (Menü) > Applications (Registerkarte) 185
- Time (Registerkarte), Settings (Menü) 16
- Trace (Unterregisterkarte), Settings (Menü) > Debugging (Registerkarte) 26
- traceroute-Befehl 30

## U

- UNIX**
  - Lesezeichen erstellen 174
- UNIX Access (Unterregisterkarte), Authorization Groups (Menü) > Files (Registerkarte) 172
- UNIX Bookmarks (Unterregisterkarte), Authorization Groups (Menü) > Files (Registerkarte) 174
- UNIX/NFS**
  - Durchsuchen von Dateien 164
  - Zugriffssteuerung 172
- URL, Zugriffsstatistik 22
- USER** (Variable)
  - in UNIX-Lesezeichen 174

- in Web-Lesezeichen 161
- in Windows-Lesezeichen 170
- User Accounts (Registerkarte), Import/Export (Menü) 60

## V

- Vermittlung 153
- Vermittlung, Anmeldeinformationen von Benutzern 10
- Verschlüsselungsstärke 10
- View (Unterregisterkarte), Settings (Menü) > Log (Registerkarte) 18

## W

- Web
  - Benutzereinstellungen für die Suche 148
  - Browsing zulassen 148
  - Lesezeichen erstellen 161
  - Navigationsprobleme 26
  - Nutzungsstatistik zu Spitzenzeiten 22
  - Serverzugriffssteuerung 158
  - Zugriffssteuerung 158
- Web Proxy (Menü)
  - Konfigurationsaufgaben 264
- Web-Agent, IVE als 123
- Webproxy, Konfigurieren von Benutzer-PCs 202
- Windows
  - Durchsuchen von Dateien 164
  - Lesezeichen erstellen 170
  - Ressourcenzugriffssteuerung 167
- Windows Access (Unterregisterkarte), Authorization Groups (Menü) > Files (Registerkarte) 167
- Windows Bookmarks (Unterregisterkarte), Authorization Groups (Menü) > Files (Registerkarte) 170
- Windows NT-Domänenserver
  - Konfigurationsschritte 106
  - Übersicht 75
- Windows-Registrierung, Änderungen 207
- WINS
  - für externen Port 241
  - für internen Port 240

## Z

- Zeit
  - Begrenzungen für
    - Administratorensitzungen 86
    - Sitzungsbegrenzungen für Benutzer 133
    - Systemzeit einstellen 16
- Zertifikat
  - Beschreibung 41
  - clientseitiges Zertifikat erforderlich 42, 52
  - Codesignatur 54
  - Einschränken von Anmeldungen
    - Administrator 91
    - Benutzer 142, 145
  - JavaSoft 54
  - MS Authenticode 54
  - Schlüssel
    - bestehenden exportieren 43
    - bestehenden importieren 43
  - Server
    - bestehendes exportieren 43
    - bestehendes importieren 43
    - erneuertes Zertifikat importieren 45
    - Zertifikatssignaturanforderung erstellen 47
  - Signaturanforderung
    - Zertifikat importieren 50
  - Stammzertifikat 52
  - unterstützte Formate 41
  - verkettet 52
- Zertifikatssignaturanforderung
  - erstellen 47
  - Zertifikat importieren 50
- Zertifikatssignaturanforderung erstellen 47
- Zugriffssteuerung
  - allgemeines Durchsuchen von Dateien 164
  - allgemeines Webbrowsing 148
  - UNIX/NFS-Ressourcen 172
  - Webressourcen 158
  - Windows-Ressourcen 167
- Zugriffssteuerungsliste (ACL)
  - exportieren 64
  - importieren 64
- Zuordnung von Benutzern zu Gruppen
  - Festlegen einer Option 92
  - Festlegen von Regeln 98
- Zuordnungen von Servern zu Gruppen 137





